



PRAVNI
FAKULTET
SVEUČILIŠTA
U SPLITU

**3rd INTERNATIONAL DOCTORAL AND
POSTDOCTORAL CONFERENCE IN THE LAW
AND LAW RELATED FIELDS "LEGAL
CHALLENGES OF ECONOMIC AND SOCIAL
DEVELOPMENT - CHALLENGES OF THE
MODERN WORLD"**

Editors:

Željka Primorac, Ranka Jeknić

BOOK OF PROCEEDINGS

Split, 13 - 14 May 2026

Faculty of Law, University of Split

**3rd INTERNATIONAL DOCTORAL AND
POSTDOCTORAL CONFERENCE IN THE LAW AND
LAW RELATED FIELDS „LEGAL CHALLENGES OF
ECONOMIC AND SOCIAL DEVELOPMENT –
CHALLENGES OF THE MODERN WORLD“ –
SPLITLAW 2026**

BOOK OF PROCEEDINGS

Editors:

Željka Primorac, Ranka Jeknić

Split, 13 - 14 May 2026

Publisher:

Faculty of Law, University of Split, Croatia

Editors in Chief

Željka Primorac, PhD., Full Professor, Faculty of Law, University of Split, Croatia

Ranka Jeknić, Phd., Assistant Professor, Faculty of Law, University of Split, Croatia

Executive Editor

Matko Pajčić, PhD., Associate Professor, Faculty of Law, University of Split, Croatia

Technical Editors

mr. sc. Ivona Matas, mag. iur., librarian, Faculty of Law, University of Split, Croatia

Tomislav Staničić, M. J., senior librarian, Faculty of Law, University of Split, Croatia

Editorial Board

Ratko Brnabić, PhD., Associate Professor, Faculty of Law, University of Split, Croatia

Marko Ivkošić, PhD., Associate Professor, Faculty of Law, University of Split, Croatia

Ines Medić, PhD., Full Professor, Faculty of Law, University of Split, Croatia

Tomaž Keresteš, PhD., Full Professor, Faculty of Law, University of Maribor, Slovenia

Vesna Rijavec, PhD., Full Professor, Faculty of Law, University of Maribor, Slovenia

Wojciech Zalewski, PhD., Associate Professor, Faculty of Law, University of Gdansk, Poland

Małgorzata Balwicka-Szczyrba, PhD., Associate Professor, Faculty of Law, University of Gdańsk, Poland

Piotr Uziębło, PhD., Associate Professor, Faculty of Law, University of Gdańsk, Poland

Victor Garcia Yzaguirre, PhD., Faculty of Law, University of Girona, Spain

Technical Board

Petar Rašetina, mag. iur., Faculty of Law, University of Split, Croatia

Ivan Mikrut, mag. iur., Faculty of Law, University of Split, Croatia

Daniela Nazor, dipl. Iur., Faculty of Law, University of Split, Croatia

**3rd INTERNATIONAL DOCTORAL AND POSTDOCTORAL
CONFERENCE IN THE LAW AND LAW RELATED FIELDS
„LEGAL CHALLENGES OF ECONOMIC AND SOCIAL
DEVELOPMENT – CHALLENGES OF THE MODERN WORLD“**

SPLITLAW 2026

ISSN (Online): 3043-9906

Publisher

Faculty of Law, University of Split, Croatia

For the publisher

Željka Primorac, PhD., Full Professor, Faculty of Law, University of Split, Croatia

Ranka Jeknić, PhD., Assistant Professor, Faculty of Law, University of Split, Croatia

Organizing Committee

Željka Primorac, PhD., Full Professor, Faculty of Law, University of Split, Croatia

(President)

Ratko Brnabić, PhD., Associate Professor, Faculty of Law, University of Split, Croatia (Co-
President)

Ines Medić, PhD., Full Professor, Faculty of Law, University of Split, Croatia

Marija Đuzel, PhD., Associate Professor, Faculty of Law, University of Split, Croatia

Marija Vidić, PhD., Associate Professor, Faculty of Law, University of Mostar, Bosnia and
Herzegovina

Tomaž Keresteš, PhD., Full Professor, Faculty of Law, University of Maribor, Slovenia

Wojciech Zalewski, PhD., Associate Professor, Faculty of Law, University of Gdansk,
Poland

Ante Šimun Majstorović, mag. iur., Faculty of Law, University of Split, Croatia

Program Committee

Ranka Jeknić, PhD., Assistant Professor, Faculty of Law, University of Split, Croatia
(President)

Maja Proso, Full Professor, Faculty of Law, University of Split, Croatia

Marko Ivkošić, PhD., Associate Professor, Faculty of Law, University of Split, Croatia

Marin Keršić, PhD., Assistant Professor, Faculty of Law, University of Split, Croatia

Ivana Radić, PhD., Assistant Professor, Faculty of Law, University of Split, Croatia

Ana Radina, Associate Professor, Faculty of Law, University of Split, Croatia

Vedran Zlatić, PhD., Assistant Professor, Faculty of Law, University of Split, Croatia

Blanka Čop, PhD., PostDoc, Faculty of Law, University of Split, Croatia

Vesna Rijavec, PhD., Full Professor, Faculty of Law, University of Maribor, Slovenia

Małgorzata Balwicka-Szczyrba, PhD., Associate Professor, Faculty of Law, University of
Gdańsk, Poland

Piotr Uziębło, PhD., Associate Professor, Faculty of Law, University of Gdańsk, Poland

Victor Garcia Yzaguirre, PhD., Faculty of Law, University of Girona, Spain

Technical Committee

Petar Rašetina, mag. iur., Faculty of Law, University of Split, Croatia

Ivan Mikrut, mag. iur., Faculty of Law, University of Split, Croatia

Daniela Nazor, dipl. Iur., Faculty of Law, University of Split, Croatia

Editors

Željka Primorac, PhD., Full Professor, Faculty of Law, University of Split, Croatia

Ranka Jeknić, PhD., Assistant Professor, Faculty of Law, University of Split, Croatia

Executive Editor

Matko Pajčić, PhD., Associate Professor, Faculty of Law, University of Split, Croatia

Review

Ines Medić, PhD., Full Professor, Faculty of Law, University of Split, Croatia

Maja Proso, Full Professor, Faculty of Law, University of Split, Croatia

Proofreading

Tania Žuvela Blažević, PhD, senior lecturer, Faculty of Law, University of Split, Croatia

Layout & Design

Ante Koštić

Print

TEHNIČAR KOPIRNI CENTAR d.o.o.

CONTENT

Foreword	III
Melinda Simonyi-Kovács	
PROHIBITION OF DOUBLE ASSESSMENT – THE PROBLEM OF TAX ADMINISTRATION PROCEEDINGS RUNNING IN PARALLEL TO CRIMINAL PROCEEDINGS	1
Andrej Bozhinovski	
PROVING INNOCENCE THROUGH NEW EVIDENCE: THE TREATMENT OF NEW EVIDENCE IN THE REOPENING OF CRIMINAL PROCEEDINGS	21
Tamás Károly Goricsán	
THOUGHTS ON THE EFFECTIVENESS OF MEASURES AGAINST MONEY LAUNDERING	43
Hrvoje Bralić	
CAUSATION IN THE CRIMINAL OFFENSE OF NEGLIGENT MEDICAL TREATMENT IN LEGAL DOCTRINE AND CROATIAN CASE LAW	67
Henrietta Németh-Kiss	
THE IMPACT OF DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE ON THE CRIMINAL LAW ASSESSMENT OF DRUG TRAFFICKING IN HUNGARY	83
Nikolina Tomaš	
FUNCTIONAL APPROACH TO THE RECOGNITION OF FAMILY RELATIONSHIPS IN THE CASE LAW OF EUROPEAN COURTS	101
Hedvig Szabó	
LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE-BASED DISINFORMATION AND DEEPFAKE TECHNOLOGIES IN THE EUROPEAN UNION PROTECTION OF DEMOCRATIC ELECTORAL PROCESSES AND THE BALANCE WITH FREEDOM OF SPEECH	129
Lisa Marie Breyer	
THE PRESUMPTION OF CONFORMITY FOR MEDICAL AI UNDER THE AI ACT: STRUCTURAL LIMITS OF MDR CONFORMITY ASSESSMENT FOR CONTINUOUS-LEARNING GENETIC DIAGNOSTIC SOFTWARE	149
Hannah Hafenscher	
CONSTITUTIONALIZING TERMS OF SERVICES? ARTICLE 14 (4) DSA AND THE BLURRING OF PUBLIC AND PRIVATE LAW IN THE EUROPEAN UNION	177

Julia Małgorzata Kalus	
DEEPFAKE – A PROBLEM ITSELF OR A SYMPTOM OF A DEEPER PROBLEM?	201
Alexandra Salnikow	
DEEPFAKES ACROSS JURISDICTIONS: REGULATORY APPROACHES IN TENNESSEE AND DENMARK TO THE PROTECTION OF PERSONAL CHARACTERISTICS.....	227
Dóra Rengel	
THE EU REGULATORY FRAMEWORK ON DEEPFAKE CHILD SEXUAL ABUSE MATERIAL: CURRENT SOLUTIONS AND FUTURE DIRECTIONS	257
Józsa Ede	
RETHINKING THE CONCEPT OF CONTRACTUAL FREEDOM IN THE ERA OF SMART CONTRACTS.....	287
Fani Milan Ostojić	
KEY CHARACTERISTICS OF THE DRAFT PROPOSAL FOR THE AMENDMENTS TO THE CONSUMER PROTECTION ACT OF 2025	307
Tea Micevska	
ILLEGALLY OBTAINED EVIDENCE IN INTERNATIONAL ARBITRATION	343
Sanja Čović Jurčević	
COSTS OF PROCEEDINGS BEFORE THE CONSTITUTIONAL COURT AND THE RIGHT OF ACCESS TO A COURT IN THE LIGHT OF ECtHR CASE LAW	361
Fines Fatimah	
SILENCING THE RAINBOW: BETWEEN MORAL PANIC AND THE RIGHT TO DEFEND SOCIAL MORALITY IN INDONESIA	389
Nguyen Thi Hang Diem Mi	
THE ACTUAL SITUATION OF VIETNAM’S GI LEGAL FRAMEWORK AND THE MEASURES FOR ITS MAINTENANCE AND DEVELOPMENT	413

FOREWORD

The 3rd International Doctoral and Postdoctoral Conference in Law and Law Related Fields "Legal Aspects of Economic and Social Development - Challenges of the Modern World." – SPLITLAW 2026, held on May 13-14, 2026 and hosted at the Faculty of Law University of Split, represents a recognized lifelong learning program of the Center for Lifelong Learning, Faculty of Law, University of Split.

Over the past three years SPLITLAW, as a special international scientific conference, has become recognized by doctoral students (PhD students) and post-doctoral students (PostDoc researchers) from the field of social sciences – law and other related fields of social sciences or interdisciplinary fields related to law. SPLITLAW 2026 had 32 presentations from 4 countries in Europe (Austria, Hungary, Croatia, Republic of North Macedonia).

The international character of the conference is strengthened by the fact that 2/3 of the participants were from abroad - Deák Ferenc Faculty of Law and Political Science, Law Doctoral School Faculty of Law - University of Pécs, Faculty of Law and Political Sciences - University of Szeged, Faculty of Law, University of Miskolc, Doctoral School of Political Science and Law - University of Debrecen, Pázmány Péter Catholic University, Faculty of Law and Political Science, Faculty of Law - University of Vienna etc.

As a President of the Organizing Committee of the SPLITLAW 2026, it is a great pleasure to present you Book of Proceedings SPLITLAW 2026 in which we publish 18 double-blind peer-reviewed papers accepted for publication and categorized as an origin scientific paper, preliminary communication, review paper and professional paper. Each accepted paper for publication was presented at the conference and represents results from various scientific researches fields including topics on legal consideration of economic contexts and application of legal solutions in practices, improvement of theoretical and practical legal problem areas, public and private law crossing paths in the EU, European approach to digital transformation, digital economy and society – benefits and potential risks of AI technology etc.

I believe that the published papers will contribute to the exchange of scientific research results of domestic and foreign PhD students and PostDoc researchers at

the international level, establishing further cooperation of young researchers through the transfer of knowledge and experience in the field of legal science.

Željka Primorac, PhD., Full Professor
President of the Organizing Committee of the SPLITLAW 2026
Vice-dean for Science and Postgraduate Studies, Faculty of Law,
University of Split, Croatia

Split, May 15, 2026.

UDK: 341.231.145 (4-67 EU : 439)

343 (4-67 EU : 439)

336.226 (4-67 EU : 439)

Review paper

Melinda Simonyi-Kovács, PhD student

Deák Ferenc Faculty of Law and Political Science, Széchenyi István University, Hungary

E-mail: drkovacs.melinda@gmail.com

ORCID-ID: 0009-0008-6624-1081

PROHIBITION OF DOUBLE ASSESSMENT – THE PROBLEM OF TAX ADMINISTRATION PROCEEDINGS RUNNING IN PARALLEL TO CRIMINAL PROCEEDINGS

ABSTRACT

The ne bis in idem principle, i.e., the prohibition of double jeopardy, is one of the cornerstones of criminal law in states based on the rule of law, ensuring that the same person cannot be held accountable or punished more than once for the same act. However, in addition to criminal proceedings for budget fraud, tax administration proceedings are often conducted in parallel, which may result in tax penalties and other financial consequences. This practice raises the question of whether the parallel application of criminal and administrative punitive sanctions results in an accumulation of liability that violates the ne bis in idem principle. The problem is particularly significant in the above area, where authorities often use a range of legal instruments to protect the state's fiscal interests. At the same time, the parallelism of sanction systems raises sensitive issues regarding legal certainty and the protection of fundamental rights, especially when tax administration sanctions can be considered punitive. This study aims to examine how tax administration and criminal proceedings related to tax law violations relate to the ne bis in idem principle. The starting point for the examination is the Hungarian Constitutional Court's relevant decisions, which provide an interpretative framework for domestic law enforcement. In addition, the study presents the leading decisions of the ECHR and ECJ, which examine the conditions under which parallel sanctions and the connection between proceedings are permissible. The article aims to explore the criteria developed by international and European courts for assessing double sanctions and how these are applied in Hungarian legal practice. Finally, the study seeks to systematize the dogmatic and practical issues arising from the constitutional assessment of parallel proceedings and sanctions in cases of budget fraud.

Keywords: *Ne bis in idem-accumulation of responsibilities-multiple sanctioning systems*

1. INTRODUCTION

In Hungary, the vast majority of criminal proceedings initiated for budget fraud are preceded by tax administration proceedings, during which the tax authority files a complaint based on evidence obtained in accordance with the provisions of Act CLI of 2017 on Tax Administration (Air.). Subsequently, the two procedures run in parallel: the tax administration procedure, which in most cases ends with the imposition of a tax penalty, and the criminal proceedings, in which the court applies criminal sanctions.

Considering that the disposition of the crime of budget fraud is a framework provision in the Criminal Code¹, which is fleshed out by the tax law norms in force, the violation of tax laws also constitutes a criminal offense if the elements of the offense defined by the Criminal Code are present. Criminal Code, a violation of tax law also constitutes a criminal offense.

The taxpayer's main procedural obligations - tax return and tax payment obligations, as well as the rules governing the allocation of tax and budgetary subsidies – are set out in the Act on the Rules of Taxation (Art.). In contrast, specific tax obligations are set out in separate provisions of tax law². Violation of the obligations set out in this Act shall result in tax administration proceedings and the imposition of tax penalties. If the violation causes financial damage to the budget through the commission of the acts described in Section 396 of the Btk, criminal liability shall also be established.

The study aims to present the areas of law governing sanctions applied in cases of violation of tax law norms, where double liability arises, to analyze the practice developed in applying the law regarding the accumulation of liability, and to present solutions aimed at eliminating this. To this end, I will use qualitative document analysis to examine the Fundamental Law, procedural laws, specific sectoral laws governing administrative sanctions, and EU legislation relevant to the issue. I intend to explore the decisions of the ECtHR, the CJEU, and the Constitutional Court in areas affected by parallel liability.

In addition, examining secondary empirical sources – relevant documents based on existing empirical research, reports by legal defense organizations, ombudsman reports, and investigations by international human rights organizations – provides

¹ The Criminal Code 2012./C. Official Gazette of Hungary 181/2012., Section 396 (hereinafter: Btk.)

² Act on the Rules of Taxation 2017./CL. Official Gazette of Hungary 192/2017., Sections 49, 58-63, 64-65 (hereinafter: Art.)

an opportunity to identify potential tensions between the normative theoretical framework and actual legal practice.

Based on all this, the ultimate goal of this paper is to formulate a legislative and law-enforcement solution to enforce the prohibition on double jeopardy.

2. THE PRINCIPLE OF *NE BIS IN IDEM* AND THE ISSUE OF CUMULATIVE LIABILITY

The principle of *ne bis in idem*, or the prohibition of double jeopardy, based on Roman law, is a cornerstone of criminal law in a state governed by the rule of law, as declared in Article XXVIII(6) of the Fundamental Law of Hungary. According to this, "Except in extraordinary cases specified by law, no one may be prosecuted or convicted for a criminal offense for which they have already been acquitted or convicted in Hungary or, within the scope specified by an international treaty or a legal act of the European Union, in another state in accordance with the law." The provision of the Fundamental Law, therefore, based on its terminology, is limited exclusively to judgments handed down by the courts, which have the sole monopoly over decisions on acquittal or conviction³. In this regard, the Supreme Court emphasizes in its decision No. Bfv.III. 1068/2021/12, that, pursuant to the above-mentioned provision of the Fundamental Law, a final judgment can only be rendered by a court decision, and an administrative decision cannot have *res judicata* effect.⁴

It is therefore clear that the principles of double jeopardy and *res judicata* are interlinked and complementary. *Res judicata* has substantive binding force, while the principle of *ne bis in idem* is linked to formal *res judicata*⁵. According to the Supreme Court's decision No. Bpkf.III. 465/2022/14, substantive *res judicata* means a decision that definitively and finally decides on the merits of the charge or the conclusion of the proceedings based on the charge⁶. Formal *res judicata*, on the other hand, is a simple binding force that only precludes the given decision from being challenged by ordinary legal remedies. In terms of their combined effect, "When a decision on the merits becomes final, it has substantive legal force, which naturally also means formal legal force and unchallengeability, and

³ Steiner, G., Budget fraud and VAT fraud in practice, Orac, Budapest 2023, p. 318.

⁴ Supreme Court Bfv.III.1068/2021/12

⁵ Szabó, J., Administrative Law Dispute versus Criminal Law, JURA, year 27, 1/2021. p. 68.

⁶ Supreme Court Bpkf.III.465/2022/14.

consequently represents a final decision on the question of guilt and on the criminal law consequences, sanctions or lack thereof."⁷

Based on the above, it appears that the *ne bis in idem* principle applies to the determination of criminal liability in the event of overlapping criminal proceedings, and disregards sanctions imposed by other branches of law – determining liability and applying legal consequences – against the same person based on the same facts.⁸ It does so even though, in Hungary, as in other Member States of the European Union, we are witnessing a spectacular rise in administrative criminal law, i.e., punitive criminal law sanctions that are not criminal, being applied more and more widely. One of the driving forces behind this trend is the goal of reducing the burden on the criminal justice system to ensure effective and timely adjudication, which is achieved by decriminalizing certain acts, i.e., removing them from the scope of criminal law. Another reason for this expansion is that legislators are seeking to ensure compliance with norms outside criminal law – mainly administrative norms, given their scope – by creating a system of sanctions characteristic of substantive and procedural criminal law, primarily in the area of investigation. The latter category also includes action against acts that damage the budget, in which case the sanctions imposed may be more severe than those applied in criminal proceedings.

However, despite or in addition to the above legislative intent, criminal proceedings may also be initiated if the violation of tax law also fulfills the elements of a criminal offense under substantive law. In such cases, therefore, the act does not remain within the territory of criminal law, but crosses over into the territory of another branch of law.⁹

In addition to the above, Section 7(5) of the Criminal Procedure Act in force states, at a fundamental level, that in the question of whether the accused has committed a criminal offense, the court, the public prosecutor's office, and the investigating authority are not bound by decisions made in civil, administrative, misdemeanor, disciplinary, or other proceedings, or by the facts established therein.¹⁰

In connection with this procedural provision, the Supreme Court explained in its aforementioned decision No. Bfv.III. 1068/2021/12, that, in determining whether

⁷ Supreme Court Decision No. 2/2015 BJE

⁸ Kis, N., Supranational sanctions in: Ferenc Kondorosi-Katalin Ligeti: Handbook of European Criminal Law, Magyar Közlöny Kiadó, Budapest 2009, p. 385.

⁹ Szabó, op. cit. note 5. p. 70.

¹⁰ Criminal Procedure Act 2017/XC. Official Gazette of Hungary 90/2017. Section 7(5) (hereinafter: Be.)

the defendant committed a criminal offense, the court is not bound by the decision made in the administrative proceedings or the facts established therein. Thus, it is legally settled that when different proceedings coincide, there should not be two other findings of fact based on the same conduct. In contrast, in the context of sentencing and sanctions, the legal consequences established for the same person for the same conduct must be taken into account.¹¹

Accordingly, other proceedings must give way to criminal proceedings to avoid differing findings of fact. Still, double sanctions are permissible under the above Supreme Court decision, and the legal consequences applied in other proceedings may only be "taken into account, considered..." The above position is consistent with the position expressed in the Supreme Court's earlier decision published under number EBD 2019.09.B16. According to the decision in the proceedings initiated for the crime of budget fraud "the tax penalty imposed in the tax proceedings does not preclude the initiation of criminal proceedings and the application of criminal sanctions for the act on which the tax penalty is based; this does not violate the prohibition of double jeopardy, but the tax penalty imposed may be relevant in the criminal proceedings."

The other side of the coin – i.e., the binding nature of the facts determined by administrative law – is that the court is not bound by the decisions of other authorities or disciplinary decisions or the facts established therein, unless the consequences of a criminal offense that has been finally adjudicated must be determined in administrative proceedings, the court cannot find that the convicted person did not commit the offense with which he or she was charged.¹² In established judicial practice, a final judgment in a criminal case is binding only on the court that adjudicates guilt in administrative proceedings, as the law expressly prohibits any other use of such judgments. However, there is no legal obstacle to the court establishing a different set of facts in an administrative case based on the evidence presented there, including other details.¹³

Thus, the court hearing the administrative case is bound by the decision of the criminal court only to the extent that it cannot establish the defendant's lack of criminal liability in the criminal proceedings, nor can it hold the acquitted person liable. At the same time, the administrative court may decide differently on other

¹¹ Supreme Court Bfv.III.1068/2021/12.

¹² Act on Administrative Procedure I /2017 Official Gazette of Hungary 13/2017. Section 85(6)(7)

¹³ Supreme Court Kfv. 35155/2004. EBH.2005.1257.

facts of the case, such as the place and time of the offense, the amount of financial loss or damage, and may establish a different set of facts.¹⁴

Comparing the regulations of the two branches of law, it can be concluded that avoiding the establishment of different facts is reduced solely to the point of liability. However, about other details of the facts, both courts may form and express their own position based on the results of the evidentiary proceedings conducted in accordance with the rules of procedure determined by their own jurisdiction, according to which they may apply sanctions in accordance with their own standards. This possibility of diversion is generally acceptable, but, for example, financial loss or damage caused by it is a crucial issue in criminal proceedings that may determine the legal classification of the offense, with implications for the severity of the sanction. At the same time, the time of commission, especially in view of frequently changing tax laws, may influence both the question of guilt and the legal consequences applied.

3. EU REGULATIONS

The Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on November 4, 1950, and promulgated by Hungary in Act XXXI of 1993¹⁵ (ECHR), declares the prohibition of double jeopardy, stipulating that "if a person has been finally acquitted or convicted by a court of a state in accordance with its criminal law and criminal procedure law in respect of a criminal offense, the judicial authorities of that State may not prosecute or punish that person for the same offense." The Convention thus enshrined the principle of double jeopardy at the international level, but limited its application to the jurisdiction of a given state.¹⁶

Article 54 of the Convention implementing the Schengen Agreement¹⁷ (CISA) regulates the principle of *ne bis in idem* in relations between Member States. According to this EU rule, "a person whose conduct has been finally judged in one of the Contracting Parties shall not be prosecuted in the territory of another

¹⁴ Szabó, J.; Molnár, D., At the intersection of constitutional law and EU law: the principle of "ne bis in idem" European Law, year 23, 4/2023, p. 14.

¹⁵ The Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on November 4, 1950, and promulgated by Hungary in Act XXXI of 1993 (ECHR), Official Gazette of Hungary 70/1993.

¹⁶ Elek, B., The emptying of the prohibition of double jeopardy – The changing case law of the European Court of Human Rights and the Court of Justice of the European Union in relation to the *ne bis in idem* principle, Criminal Law Review year 11, 2/2022, p. 19.

¹⁷ Convention implementing the Schengen Agreement promulgated by Hungary in Act LXXXIX. of 2007 (CISA), Official Gazette of Hungary 87/2007.

Contracting Party for the same acts if the penalty has already been enforced, is currently being enforced, or can no longer be enforced under the law of *the* Contracting Party where the judgment was delivered."

According to Article 50 of the Charter of Fundamental Rights of the European Union (2007/C 303/01)¹⁸, no one shall be liable to be tried or punished again in criminal proceedings for an offense for which he or she has already been finally acquitted or convicted in accordance with the law in the Union.

In the context of the principle of *ne bis in idem*, we can see that all of the above-mentioned basic documents refer to criminal proceedings based on the same facts, brought against the same defendant, and concluded with a final decision. At the same time, both the ECtHR and the CJEU have examined punitive sanctions imposed in administrative proceedings in several cases and have found that, in the same set of facts, the parallel application of criminal and administrative sanctions may violate the prohibition of double jeopardy.¹⁹

3.1. The practice of the European Court of Human Rights

In this regard, the set of criteria used as a benchmark for determining the punitive nature of individual (administrative) sanctions was developed by the ECtHR in the case of *Engel and Others v. the Netherlands* (Engel criteria).²⁰ According to these criteria, the following aspects must be taken into account:

- the classification of the offense by the Member State concerned,
- the nature of the offense,
- the severity and nature of the penalty imposed.

According to the first criterion, if the national legislature classifies an act as a criminal offense, it is also a criminal offense under Article 6. However, if the conduct in question is not punishable under criminal law, the other two criteria must be examined. If these criteria are met, infringements that do not fall within the scope of criminal law must also be considered criminal matters under national law if they concern a violation of rules for which the state imposes legal

¹⁸ Charter of Fundamental Rights of the European Union (2007/C 303/01) Official Gazette of the European Union 30.3.2010.

¹⁹ Figula I.; - Elek, B., Thoughts on the judgment of the Court of Justice of the European Union in Case C-524/15 from an administrative and criminal law perspective. <http://ejszh.justice.hu/blog/20180503/figula-ildiko-elek-balazs-gondolatok-az-europai-unio-birosaga-c-52415-szamu-ugyenben>, 19 September 2024.

²⁰ *Engel and Others v. the Netherlands* (No.5100/71, 5101/71, 5102/71, 5354/72, 5370/72, June 8, 1976)

consequences in 'criminal' proceedings due to their nature and/or the sanctions involved.²¹ (This corresponds to the system of administrative criminal law.)

The second condition is the nature of the infringing act. When examining this, several additional circumstances must be taken into account, as the ECtHR has identified in subsequent judgments. Thus, the fundamental question is whether the legal norm referred to is of general application or applies only to a limited group.²² Is the procedure carried out by an organ of the state vested with public authority?²³ The purpose of the legal provision referred to must be to impose a general obligation that has a deterrent effect.²⁴ In addition, it must be taken into account whether the legal consequences are based on fault or objective liability, and how the issue in question is regulated in the other member states. Thus, based on this criterion, only proceedings initiated under rules binding on everyone and providing for punitive sanctions for their violation are considered criminal cases. (Such are the legal consequences applied in tax administration proceedings in the event of a breach of tax law norms.)

The third condition is the severity and nature of the punishment imposed. If the legal consequences have a profound impact on the person concerned (such as deprivation of liberty, prohibition from engaging in certain activities, or a hefty fine), the case must be treated as a criminal matter even if the regulation in question only applies to a specific group and therefore does not meet the criteria set out in the second criterion.²⁵ Thus, the combined effect of the last two conditions must also be examined. According to the ECtHR's practice, therefore, in each case the circumstances must be assessed individually to determine whether the subject matter of the proceedings is a criminal matter within the meaning of the Convention.

Following the initial judgments, which contained guarantees ensuring the strict protection of fundamental rights, both the ECtHR and the CJEU have gradually softened their practice and shown tolerance toward parallel proceedings (conducted by separate jurisdictions) in their decisions.

In the case of *Franz Fischer v. Austria*, the ECtHR ruled on parallel proceedings for traffic offenses and administrative offenses.²⁶ The applicant was sentenced to

²¹ Dudás, D., Human Rights in the Practice of the ECtHR II. – The Right to a Fair Trial <https://jogaszvilag.hu/szakma/emberi-jogok-az-ejeb-gyakorlatban-ii-a-tizstesseges-eljarashoz-valo-jog/6> February 2026.

²² Bendenoun v. France (No.12547/86, February 24, 1994)

²³ Benham v. United Kingdom (No.19380/92, June 10, 1996)

²⁴ Öztürk v. Germany, (No. 8544/79, February 21, 1984)

²⁵ Kapetanios and Others v. Greece, (No. 3453/12, 42941/12 and 9028/13, April 30, 2015)

²⁶ Franz Fischer v. Austria (No. 38275/97, May 30, 2002)

imprisonment for hit-and-run under the Austrian Criminal Code, while under the Traffic Act, he was also fined for causing a fatal accident while driving under the influence of alcohol. In its decision, the ECtHR found Austria violated Article 4 of Protocol No. 7 to the ECHR. The core of the judgment is that, according to the correct interpretation of the article, double jeopardy for the same criminal conduct is prohibited.²⁷

In the case of *Sergey Zolotukhin v. Russia*, the ECtHR also found a violation of Article 4 of Protocol No. 7 to the ECHR, noting that sanctions had been imposed on the applicant in two proceedings based on the same facts. (According to the facts underlying the proceedings, measures were taken against the intoxicated applicant, during which he insulted and made life-threatening threats against the members of the authority conducting the proceedings against him and attempted to escape. Because of his behavior, he was detained in administrative proceedings and then convicted in criminal proceedings.²⁸

In the case of *Dungeveckis v. Lithuania*,²⁹ the ECtHR summarized its practice to date and found that there is a violation of Article 4 of Protocol No. 7 to the ECHR if the applicant's responsibility has been previously decided by a final decision (whether a conviction or acquittal), two proceedings were conducted against him, both of which were criminal in nature and both of which were based on the same facts.

In *Grande Stevens and Others v. Italy*,³⁰ the ECtHR examined the criminal nature of market surveillance sanctions imposed by the Italian Securities and Exchange Commission. In this case, the administrative authority took action against three natural persons and two companies, imposing fines, and subsequently filed a complaint, which led to criminal charges being brought on the same facts. The national court did not accept the applicants' reference to the violation of the *ne bis in idem* principle, so they turned to the ECtHR, referring to Article 4 of Protocol No. 7 to the Convention, which, referring to the Engel criteria, found that although the administrative proceedings under national law were not criminal, the legal disadvantage applied (a fine close to the maximum amount) was of such a magnitude that it satisfied the criteria set out in the Engel judgment about sanctions. Neither the procedure applied nor the fine was intended as a reparation,

²⁷ Ambrus, I., The *ne bis in idem* principle in recent European case law, with an overview of the application of the principle in cases where different areas of law intersect. *European Mirror*, year 22, 3/2019. p. 127.

²⁸ *Sergey Zolotukhin v. Russia* (No. 14939/03, February 10, 2009)

²⁹ *Dungeveckis v. Lithuania* (No. 32106/08, April 12, 2016)

³⁰ *Grande Stevens and Others v. Italy* (No. 18.640/10, 18.647/10, 18.663/10, March 4, 2014)

but served a specific preventive purpose. The Court therefore also condemned the Italian State for violating the principles of fair trial and *ne bis in idem*.

In its judgments in *Västberga Taxi Aktiebolag and Vulic v. Sweden*³¹ and *Janosevic v. Sweden*, the ECtHR applied the Engel criteria relating to sanctions to the imposition of tax penalties based on the above reasoning and found that such legal consequences comply with the conditions for "criminal" sanctions under Articles 6 and 7 of the ECHR and Article 4 of Protocol No. 7.

However, the Court took a contrary position in *A and B v. Norway*.³² According to the above judgment of the ECtHR, in the case of "pro forma" administrative sanctions that meet the Engel criteria, the parallel conduct of criminal and administrative proceedings and the application of legal consequences do not violate the *ne bis in idem* principle if there is a sufficiently close connection between the proceedings governed by the two branches of law in terms of subject matter and time, and if they do not repeat but complement each other. Therefore, if the parallel proceedings form a coherent whole and appear to be part of a single proceeding in that they examine different aspects of it, the *ne bis in idem* principle is not violated.³³ The ECtHR has also developed a set of conditions for this, according to which:

- The complementary function of the proceedings should not be merely theoretical, but should specifically concern different segments of the act in question.
- The consequences should be foreseeable.
- Duplication should be avoided when gathering and evaluating evidence
- The sanction imposed in the previous proceedings must be taken into account in subsequent proceedings (requirement of proportionality).

In the above case, the ECtHR adopts a solution contrary to its previous practice, grounded in the theoretical basis that different proceedings and the sanctions imposed in them may serve various purposes, which may complement each other (the "integrated whole" of the proceedings). If these conditions are met, no violation of the *ne bis in idem* principle can be established. According to Lárís Liliána, with whom I agree, "this decision of the ECtHR is debatable, as it has expanded the concept of the *ne bis in idem* principle with an element that leaves the requirement of proportionality as the only limitation on multiple proceedings."³⁴

³¹ *Västberga Taxi Aktiebolag and Vulic v. Sweden* (No. 36985/97. July 23, 2002)

³² *A and B v. Norway* (No. 24130/11, 29758/11. November 15, 2016)

³³ Elek. op. cit. note 16, p. 20.

³⁴ Lárís, L., New directions in the interpretation of the prohibition of double assessment. *Prosecutors' Journal*, year 25, 6/2018. p.110.

3.2. The practice of the Court of Justice of the European Union

The violation of the prohibition on double assessment in the CJEU's practice, compared with that of the ECtHR, arose later. Still, at that time the Court of Justice of the European Union ruled in favor of the cumulative nature of the proceedings, referring to the ECtHR's "newly established practice."³⁵ In connection with Article 50 of the Charter of Fundamental Rights, it was necessary to define the concept of "criminal offense," which the CJEU provided in Case C-489/10 Bonda³⁶. In its judgment, the Court referred to the Engel criteria as a benchmark and considered the classification under domestic law, the nature of the infringement, and the nature and severity of the penalty that could be imposed on the person concerned to be fundamental considerations.

In Case C-617/10 Fransson³⁷, which concerned the examination of tax and criminal proceedings in connection with a failure to comply with value added tax return obligations, the CJEU ruled that it is possible to conduct both criminal and administrative proceedings based on the same facts and, depending on the outcome of those proceedings, to impose both types of penalty, provided that the administrative penalty is not of a criminal nature. Based on the interpretation of Article 50 of the Charter, the sanction provided for by administrative law cannot be applied concurrently with the sanction applicable in criminal proceedings if the latter is criminal and has already become final.

In Case C-524/15 Menci³⁸, the CJEU ruled that the *ne bis in idem* principle applies to national legislation under which criminal proceedings may be brought against a person who has already been definitively imposed a criminal administrative penalty within the meaning of Article 50. However, the CJEU laid down conditions for this, namely that such legislation must serve an objective that justifies the accumulation of proceedings and penalties (in this case, the fight against VAT infringements) it must contain rules ensuring that the accumulation of procedures is limited to what is strictly necessary to avoid imposing an additional burden on the person concerned, and the total weight of the penalties imposed must be limited to what is strictly necessary in relation to the seriousness of the infringement committed.

³⁵ Opinion of Advocate General Manuel Campos Sánchez-Bordona <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:62015CC0524&from=HU>, Date of presentation: September 12, 2017. 24 October, 2024.

³⁶ Case C-489/10 Bonda (June 5, 2012, paras 27-28, 36, 46)

³⁷ Case C-617/10 Fransson (February 26, 2013, paras 24-25, 34-37)

³⁸ Case C-524/15 Menci (March 20, 2018, paras 9, 26, 30-31, 63-64)

In the *Garlsson Real Estate SA*³⁹ and *Enzo di Puma*⁴⁰ cases, the Court continues to follow the line of reasoning established in the *Menci* case. Elaborating on the interpretation of the principle of proportionality, it found that national legislation that allows the imposition of a criminal fine following a conviction is contrary to Article 50 of the Charter if the sentence alone is sufficient to constitute an effective, proportionate, and dissuasive punishment for the offense committed. In other words, administrative proceedings before criminal proceedings may be conducted lawfully in all cases, while the reverse – although it constitutes a restriction of the *ne bis in idem* principle – may be examined by means of a proportionality test. In other words, about double proceedings, national courts need only ensure that the additional burden actually imposed on the defendant/client as a result of the accumulation of sanctions is not excessive in relation to the seriousness of the offense committed.⁴¹

After this, it is not surprising how the European Parliament and the Council rule on the accumulation of forms of liability (Directive 2017/1371 of July 5, 2017, on the fight against fraud affecting the Union's financial interests by means of criminal law)⁴². The preamble settles the issue as follows: "Member States may, in principle, continue to apply administrative measures and sanctions in parallel in the area covered by this Directive. However, when applying the national legislation transposing this Directive, Member States shall ensure that the imposition of criminal sanctions in accordance with this Directive and the application of administrative measures and sanctions do not lead to a breach of the provisions of the Charter."

The Directive, therefore, allows for the parallel application of administrative and criminal sanctions in the area it regulates. However, Member States are required to ensure that the appropriate and practical application of "administrative measures, sanctions and fines not equivalent to criminal proceedings" laid down in EU law or in national implementing provisions is not unduly affected by criminal proceedings conducted in accordance with national law.⁴³

³⁹ Case C-537/16, *Garlsson Real Estate SA* (March 20, 2018, paras 28-29, 48)

⁴⁰ Cases C-596/16 and C-597/16. *Enzo di Puma Joined* (March 20, 2018, paras 18, 42-46)

⁴¹ Szabó, op. cit. note 5. p. 76.

⁴² The European Parliament and the Council rule on the accumulation of forms of liability (Directive 2017/1371 of July 5, 2017, on the fight against fraud affecting the Union's financial interests by means of criminal law) Official Gazette of the European Union 198, 2017.7.28. (hereinafter: PIF Directive)

⁴³ Art 14 of PIF Directive

4. HUNGARIAN LEGAL PRACTICE

Regarding the parallelism between tax administration and criminal proceedings, both the Constitutional Court's decisions and the Supreme Court's practice align with the new approach of the ECtHR and the CJEU. The Constitutional Court has addressed the nature of administrative sanctions in several of its decisions. It reviewed the system of administrative sanctions in Decision 17/2019. (V. 30.) AB.⁴⁴ According to this, their common feature is that they are based on statutory regulations and are therefore sector-specific. However, depending on the purpose of the sanction, we can distinguish between reparative and repressive sanctions, or between mixed sanctions. The former aims to restore the violated legal order, while the latter seeks to prevent it. In addition, sanctions can also be classified in objective and subjective terms. The former are those that can be imposed regardless of culpability, while the latter are linked to the state of mind, i.e., intentional or negligent. Regarding administrative sanctions, the decision states that, in most cases, they are objective in nature, referring to sewerage fines⁴⁵ and non-tax late payment⁴⁶ penalties. In contrast, the two penalties applied in the tax penalty system – tax penalties and default penalties – were classified as penalties serving both subjective and repressive purposes in accordance with the above general principles.

In interpreting the *ne bis in idem* principle, the Constitutional Court analyzed the difference between the absolute and relative purposes of administrative sanctions. In its decision No. 8/2017. (IV. 18.) It explained that administrative substantive law carries the conduct expected by the state, thus administrative sanctions are the legal consequences of an objective violation of this obligation. This is the absolute purpose of administrative sanctions, which distinguishes them from criminal sanctions based on guilt.⁴⁷

The Constitutional Court – exhaustively examining the factual elements of the offense of illegal fishing and analyzing the issue of double jeopardy for conduct also sanctioned by Act CII of 2013 on fish management and protection – ruled in Decision 18/2022. (VIII. 1.) AB found that the previous regulation violated the principles of legal certainty and *ne bis in idem*. It found that the fish protection administrative procedure and the fish protection fines and disqualifications applicable therein are punitive in nature, as they are not primarily aimed at providing financial compensation for the unlawful conduct committed or at

⁴⁴ Decision 17/2019.(V.30.) [88]– [94]

⁴⁵ Decision 5/2017 (III. 10.) AB

⁴⁶ Decision 3353/2017 (XII. 22.) AB

⁴⁷ Decision 8/2017 (IV. 18.) AB [82]

encouraging lawful conduct, but instead represent retribution for the infringement already committed, i.e. a repressive sanction that imposes a financial burden on the perpetrator of the unlawful act for preventive purposes.⁴⁸ Furthermore, neither the provisions of the Criminal Code nor those of the Hhvtv. contain any rule that would provide a guarantee against the doubling of criminal sanctions. [109]

In its decision 8/2017. (IV. 18.) AB, the Constitutional Court ruled that if criminal liability is established for the offense or crime of animal cruelty, or if a final conviction has already been handed down in the matter of criminal liability, then in animal protection proceedings initiated based on the same facts, an animal protection fine may not be imposed on the same person for the same unlawful act. At the same time, the decision also states that the provisions of the Fundamental Law do not generally preclude the legislator from attaching legal consequences belonging to other branches of law to punishable acts, in addition to criminal sanctions. In accordance with the principle of legal certainty, however, the Constitutional Court imposes on the legislator the requirement that, if an unlawful act punishable under criminal law is also subject to legal consequences under other branches of law, the relationship between the various procedures must be regulated in sufficient detail and with enough clarity. This expectation is fundamental in criminal law and procedures involving punitive sanctions, as the possibility of double punishment may arise in such contexts.⁴⁹

Animal protection fines are a regular topic of discussion for the body. Decision 13/2024. (V. 30.) AB, which divided the constitutional judges somewhat, found that the legislative omission in connection with Section 44(2) of Act XXVIII of 1998 on the protection and welfare of animals was unconstitutional, declaring that the legislature had failed to regulate the legal conditions for civil proceedings for violations of animal welfare and protection laws in accordance with the *ne bis in idem* principle in cases where criminal proceedings or animal protection proceedings by the authorities are also appropriate. The reasoning is practically parallel to that contained in Decision 18/2022. (VIII. 1.) AB.

If we analyze the provisions of Section 170(1), according to which the tax penalty is 200% of the tax shortfall if the tax shortfall is related to the concealment of income, the falsification or destruction of documents, books, or records, we can see that this sanction is by no means based on objective liability. This legal consequence is subjective and based on culpability. It applies precisely to conduct that is also punishable under criminal law. At the same time, in relation to tax and

⁴⁸ Decision 18/2022 (VIII. 1.) AB [85]

⁴⁹ Decision 8/2017 (IV. 18.) AB [49]

criminal proceedings, the Constitutional Court does not impose a prohibition, unlike in cases involving animal protection fines or illegal fishing.

Point III/9 of Opinion 56 BK of the Supreme Court states that, when imposing a sentence, it should be taken into account that the offender may suffer other actual disadvantages in addition to the criminal law disadvantages resulting from the offense. If these can have a deterrent effect in addition to the punishment, they constitute mitigating circumstances.⁵⁰

This line of reasoning is further developed in the decisions of the Supreme Court, which consistently follow the practice of the ECtHR and the CJEU of allowing the accumulation of liability, with the only limitation being proportionality from the perspective of the *ne bis in idem* principle. "It follows from all this that in criminal proceedings initiated for budget fraud, the facts established by the court must necessarily refer to the data of the proceedings that can be assessed in the context of the identity of the act in the administrative proceedings, so that if the administrative authority has imposed a sanction on the defendant in administrative proceedings for the same act, these facts must necessarily be recorded, and if there is data available, the amounts paid as a result of the administrative sanction in the administrative proceedings must also be recorded."

According to the decision of the highest judicial forum in the matter of insider trading, when imposing penalties, it is possible to eliminate the disadvantages that would otherwise be imposed on the defendant due to the accumulation of proceedings and the imposition of administrative sanctions on the defendant, while ensuring that the sanctions imposed are commensurate with the seriousness of the offense committed.⁵¹ Therefore, it is the task of the courts hearing criminal cases to impose a proportionate penalty, taking into account the range of penalties provided for in the Criminal Code and other factors affecting penalty imposition, while also considering the administrative sanctions imposed on the defendant for the same facts.

5. CONCLUSION

Nowadays, we can observe the spread of administrative criminal law in Hungary. One of the driving forces behind this is the goal of reducing the burden on the criminal justice system through legislation and court action to establish and

⁵⁰ Supreme Court EBD 2019.09.B16

⁵¹ Supreme Court Bfv.III.1068/2021/12.

maintain effective, timely adjudication, while also creating a faster, simpler system of sanctions for violations of administrative norms.

However, the concept of administrative sanctions has not been precisely defined either in Hungary or in the European Union, and individual states apply this system to varying degrees. Some countries reject the legitimacy of administrative criminal law altogether, while others regulate it in a uniform substantive and procedural law. Countries that take an intermediate approach, such as Hungary, lack a uniform legal basis or sanctions system.

Administrative criminal law raises constitutional concerns regarding cumulative liability when applied in parallel with criminal proceedings in cases involving liability for conduct prohibited by substantive criminal law.

Both international courts and, accordingly, Hungarian case law have developed over the past decade at the expense of the prohibition of double assessment. The initial strict standards of the ECtHR have now been completely relaxed, and only the overall proportionality of legal consequences remains as a limitation on parallel proceedings.

In these cases, the fundamental rights of individuals are weighed against public interests such as the enforcement of the state's criminal power, financial interests related to tax revenues, the possibility and need for effective action against crimes affecting budgets, often across national borders, and the preventive factor. In my opinion, the relationship between tax administration proceedings and criminal proceedings – as is genuine for all proceedings in the field of administrative criminal law – should be regulated at the legislative level. A choice should be made between the different regulatory approaches in accordance with the state's legal policy interests: whether to exclude the possibility of double jeopardy, thereby extending the *ne bis in idem* principle beyond criminal law to identical facts, or to allow for parallel proceedings, but in this case, it provides legal guarantees to the individual and does not rely solely on "contingent" judicial discretion to provide legal protection.

A dual system of proceedings can be observed in many European countries. Still, several states, recognizing the constitutional concerns, have introduced appropriate regulations to ensure the application of proportionate legal consequences. Thus, according to the French solution, the two penalties together may not exceed the more severe penalty applicable to individual infringements. German case law applies a proportionality criterion in each case to avoid excessive accumulation of sanctions, while in Sweden, the severity of the sanction imposed

in criminal proceedings may be reduced by the legal consequences imposed in an administrative decision. However, there are also regulatory solutions, such as the Spanish model, under which, if criminal proceedings are initiated, the authority conducting the administrative proceedings must suspend the case until the criminal court issues a final decision.⁵²

The legal definition of the crime of budget fraud in Section 396(8) allows⁵³ for unlimited mitigation if the defendant compensates for the financial loss caused by the budget fraud before the indictment. However, this provision applies to the payment of financial losses established in criminal proceedings; the Criminal Code does not mention tax penalties imposed in tax administration proceedings and their enforcement. In addition, in many cases, tax administration proceedings initiated before criminal proceedings are concluded later, due to the exhaustion of legal remedies, so the outcome is not yet known when applying the criminal law consequences. At the same time, neither the suspended nor the enforceable prison sentence imposed in the criminal case, nor the imposition of a tax penalty of up to 200%, deters the authority conducting the tax administration proceedings. Thus, in my opinion, the criterion of proportionality, i.e., the examination of whether the legal consequences applied jointly and severally are proportionate, is lost.

Although the Supreme Court's above-mentioned decisions clearly require criminal courts to consider the outcome of tax administration proceedings, this is often not possible due to the specific nature of those proceedings. Furthermore, I think it is questionable to assess whether a set of sanctions is proportionate in a given case, as this is a matter of subjective judgment, as differences in individual assessments may yield different outcomes for the same case.

In view of the changing practices of the ECtHR, the CJEU, and the Constitutional Court, as well as the uncertainty inherent in decisions based on subjective considerations, and in agreement with the ideas expressed by Professor Norbert Kis nearly ten years ago, "legislation must put the drafting of a framework law on administrative penalties on the agenda. The code must regulate the general substantive and procedural principles of repressive sanctions falling within the

⁵² Elek, op cit. note 16. p. 21.

⁵³ Btk. Section 396(8) The penalty may be mitigated without limitation if the person who caused the financial loss specified in paragraphs (1) to (6) by means of budget fraud compensates for the loss before the indictment is filed. This provision shall not apply if the offense is committed in a criminal conspiracy, criminal organization, or as a repeat offender.

competence of administrative authorities.”⁵⁴ (Although the Sanctions Act⁵⁵ has since been enacted, it does not have general validity.) In addition to the demands made on the legislator, the relationship between administrative criminal law and criminal law, the hierarchy of the two procedural systems, the combined and absolute legal consequences applied in each procedure, and, last but not least, the consistency of the dual sanctioning system with fundamental legal principles should also be formulated at the legislative level, as this would best serve the requirements of the rule of law and legal certainty.

REFERENCES

BOOKS AND ARTICLES

1. Ambrus, I., *The principle of ne bis in idem in recent European case law, with an overview of the application of the principle in cases where different areas of law intersect*, European Mirror, year 22, 3/2019, p.122-135.
2. Elek, B., *The hollowing out of the prohibition of double jeopardy – The changing case law of the European Court of Human Rights and the Court of Justice of the European Union in relation to the ne bis in idem principle*, Büntetőjogi Szemle year 11, 2/2022, p. 18-24.
3. Kis, N., *The dilemmas of administrative criminal power in terms of effectiveness and legal certainty*. Belügyi Szemle year 63, 12/2015, p. 49-68.
4. Kis, N., *Supranational sanctions* /Kondorosi Ferenc-Ligeti Katalin: Handbook of European Criminal Law, Magyar Közlöny Kiadó, 2009.
5. Lárís, L., *New directions in the interpretation of the prohibition of double jeopardy*. Ügyészek Lapja, year 25, 6/2018, p.109-121.
6. Steiner, G., *Budget fraud and VAT fraud in practice*, Orac, Budapest 2023.
7. Szabó, J.; Molnár, D., *At the intersection of constitutional law and EU law: the principle of "ne bis in idem"*, European Law, year 23, 4/2023, p.13-19.
8. Szabó, J., *Administrative law disputes versus criminal law*, JURA, year 27, 1/2021, p.67-85.

⁵⁴ Kis, N., *The dilemmas of administrative criminal power in terms of effectiveness and legal certainty*. Belügyi Szemle, year 63, 12/ 2015, p. 66.

⁵⁵ Act on sanctions for administrative violations CXXV/2017, Official Gazette of Hungary 171/2017.

LEGAL ACTS

1. Act on Administrative Procedure 2017/I Official Gazette of Hungary 13/2017.
2. Act on sanctions for administrative violations 2017/ CXXV, Official Gazette of Hungary 171/2017.
3. Act on the Rules of Taxation 2017/CL. Official Gazette of Hungary 192/2017.
4. Charter of Fundamental Rights of the European Union (2007/C 303/01) Official Gazette of the European Union 30.3.2010.
5. Convention implementing the Schengen Agreement promulgated by Hungary in Act LXXXIX. of 2007 (CISA), Official Journal of Gazette 87/2007.
6. Fundamental Law of Hungary 2011/XCIII. Official Gazette of Hungary 43/2011.
7. The Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on November 4, 1950, and promulgated by Hungary in Act XXXI of 1993 (ECHR), Official Gazette of Hungary 70/1993.
8. The Criminal Code 2012/C. Official Gazette of Hungary 181/2012.
9. The Criminal Procedure Act 2017/XC. Official Gazette of Hungary 90/2017.
10. The European Parliament and the Council rule on the accumulation of forms of liability (Directive 2017/1371 of July 5, 2017, on the fight against fraud affecting the Union's financial interests by means of criminal law) Official Gazette of the European Union 198, 28/7/2017

COURT PRACTICE

1. *A and B v. Norway* (No. 24130/11, 29758/11. November 15, 2016)
2. *Bendenoun v. France* (No.12547/86, February 24, 1994)
3. *Benham v. United Kingdom* (No.19380/92, June 10, 1996)
4. *Dungveckis v. Lithuania* (No. 32106/08, April 12, 2016)
Engel and Others v. the Netherlands (No.5100/71, 5101/71, 5102/71, 5354/72, 5370/72, June 8, 1976)
5. *Franz Fischer v. Austria* (No. 38275/97, May 30, 2002)
6. *Grande Stevens and Others v. Italy* (No. 18.640/10, 18.647/10, 18.663/10, March 4, 2014)
7. *Kapetanios and Others v. Greece* (No. 3453/12, 42941/12 and 9028/13, April 30, 2015)
8. *Öztürk v. Germany*, (No.8544/79, February 21, 1984)

9. *Sergey Zolotukhin v. Russia* (No. 14939/03, February 10, 2009)
10. *Västberga Taxi Aktiebolag and Vulic v. Sweden* (No. 36985/97. July 23, 2002.
11. Case C-489/10 Bonda (June 5, 2012, paras 27-28, 36, 46)
12. Case C-617/10 Fransson (February 26, 2013, paras 24-25, 34-37)
13. Case C-524/15 Menci (March 20, 2018, paras 9, 26, 30-31, 63-64)
14. Case C-537/16, Garlsson Real Estate SA (March 20, 2018, paras 28-29, 48)
15. Cases C-596/16 and C-597/16. Enzo di Puma Joined (March 20, 2018, paras 18, 42-46)
16. Constitutional Court Decision 5/2017 (III. 10.) AB
17. Constitutional Court Decision 3353/2017 (XII. 22.) AB
18. Constitutional Court Decision 8/2017 (IV. 18.) AB
19. Constitutional Court Decision 18/2022 (VIII. 1.) AB
20. Constitutional Court Decision 8/2017 (IV. 18.) AB
21. Constitutional Court Decision 17/2019.(V.30.) AB
22. Supreme Court Bfv.III. 1068/2021/12
23. Supreme Court Bpkf.III. 465/2022/14.
24. Supreme Court Decision No. 2/2015 BJE
25. Supreme Court Bfv.III. 1068/2021/12
26. Supreme Court Kfv. 35155/2004. EBH.2005.1257.
27. Supreme Court EBD 2019.09.B16
28. Supreme Court Bfv.III. 1068/2021/12.
29. Supreme Court Opinion 56 BK
30. Supreme Court EBD 2019.09.B.16

NETWORK RESOURCES

1. Dudás,D., Human Rights in the Practice of the ECtHR II – The Right to a Fair Trial <https://jogaszvilag.hu/szakma/emberi-jogok-az-ejebgyakorlatban-ii-a-tisztessages-eljarashoz-valo-jog/> 6. February 2026.
2. Figula, I., - Elek, B., Thoughts on the judgment of the Court of Justice of the European Union in Case C-524/15 from an administrative and criminal law perspective. <http://ejszh.justice.hu/blog/20180503/figula-ildiko-elek-balazs-gondolatok-az-europai-unio-birosaga-c-52415-szamu-ugyben> 19. September 2024.
3. Opinion of Advocate General Manuel Campos Sánchez-Bordona <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:62015CC0524&from=HU>, 24. October 2024.

UDK: 343.157 (497.5)

343.14 (497.5)

Review paper

Andrej Bozhinovski, PhD student

Faculty of Law, University of Zagreb, Croatia

E-mail: Abozinovski1@pravo.hr

ORCID ID: 0000-0003-4767-5227

PROVING INNOCENCE THROUGH NEW EVIDENCE: THE TREATMENT OF NEW EVIDENCE IN THE REOPENING OF CRIMINAL PROCEEDINGS*

ABSTRACT

This article focuses exclusively on the reopening of criminal proceedings as an avenue to prove innocence. Within that scope, it examines how new evidence, with particular emphasis on new scientific methods, is defined and assessed in U.S. and European practice. It then turns to Croatia, where it outlines the reopening procedure, the applicable standards for new evidence, and the institutional roles involved, before analysing two Croatian cases in which courts evaluated new scientific findings. Methodologically, the article combines legal analysis of the applicable rules on reopening of criminal proceedings, a comparative analysis of selected standards governing the evaluation of new scientific evidence, and case analysis. It concludes with proposals aimed at strengthening the Croatian approach so that genuine innocence claims are not blocked by an overly restrictive gatekeeping approach by the courts.

Keywords: *Innocence, reopening of the criminal procedure, scientific evidence, Croatia*

1. INTRODUCTION

You can go to prison, even though you are innocent. It really can happen to you! This is how Justin Brooks, the Director of California Innocence Project, started his lecture a year ago, which inspired me to analyze and publish this paper. Proving innocence is very hard and different sort of procedure. As academics, we analyze and scrutinize the criminal procedure, the fair trial rights, the limitation of freedom, equality of arms, etc. However, it must be noted, that during the criminal procedure, the burden of proof is on the prosecution, and the presumption of innocence is on the defendant. In proceedings after the finality of the judgement,

it is the judgment (or the system) that enjoys trust, and is presumed trusted, not the convicted person.

Once convicted, the only legal remedy to prove innocence is reopening of the criminal procedure.¹ However, how can a reopening be obtained? Well, most laws, first prescribe that you must prove that the prosecutor, or the judge, or the expert or the witness committed a criminal act (official misconduct), false testimony/expertise. Ok, what is their second option? Their second option as prescribed by law is to present new evidence which will determine that the court made a mistake *error facti*. However, if you are innocent, you need to prove that you are actually innocent, meaning you had nothing to do with the crime, not procedurally innocent (some procedural right was violated, such as, for example, not being properly summoned to a second instance hearing). That is not actual innocence. Perfect, this sounds promising. Reopening is the avenue to be pursued. However, now we get to the point where more complex questions need to be answered. First, what constitutes a new evidence? Second, can a changed testimony be considered as new evidence? Third, if there is a new scientific method to retest the evidence, developed after the trial, does that constitute new evidence? Fourth, what is the admissibility threshold of new evidence? Once the wrongfully convicted has the answers to these questions, they can proceed to the more practical; does the convicted have the same equality of arms standards as the prosecutor, the meaning of unlimited funds, team of researchers, investigators, position of power, trust by the state, forensic laboratory? Of course the answer is no. The convicted person does not even have the liberty to move freely (they are in prison), or the financial liberty to order new expertise.

* This paper is a result of research under the Project for the Career Development of Young Researchers – Training of New Doctoral Researchers (DOK-2021-02-5858), also funded by the Croatian Science Foundation (HRZZ).

¹ Although there are other extraordinary legal remedies, only reopening has been recognized as an avenue to prove substantive innocence. Croatian legislation, as well as the regional legislations have the Request for Protection of the Legality as an extraordinary legal remedy. This remedy is also not discussed here. It is an opinion of this author, that such a remedy is illogical with the new concept of adversarial or mixed procedure because it presumes that the prosecutor, apart from being a party to the procedure and has an interest in the case, at some point, will put his interest aside, and put on a cap of some kind of ombudsman of the procedure to protect procedural right the defendant. Further, only the prosecutor has the right to file a motion to the Supreme Court for such a remedy, and the defendant does not. He/she needs to request it from the prosecutor, which is illogical. The regular court and the presiding panel of judges/judge are the ones who are bound by duty and law to care about the correctness of the procedure, and the correct application of the law. However, this is a material for another article.

Bearing in mind the previous research conducted on wrongful conviction in Croatia covered rights of the wrongfully convicted people², Innocence Projects and Wrongful Convictions and other crucial perspectives.³ The aim of the article is to assess and conclude how new scientific methods are accepted as new evidence, and how new evidence thresholds are defined as opposed to Croatia, and offer practical recommendations on improving the Croatian legal framework and practice.

This article focuses exclusively on the reopening of criminal proceedings as an avenue to prove innocence. Within that scope, it examines how new evidence, with particular emphasis on new scientific methods, is defined and assessed in U.S. and European practice. It then turns to Croatia where it will outline the reopening procedure, the applicable standards for new evidence, and the institutional roles involved, before analyzing two Croatian cases in which courts evaluated new scientific findings. From the methodological approach, this article conducts legal analysis of the applicable standards on the reopening of the criminal procedure, the comparative approach to selected standards on evaluating new scientific evidence, and case analysis. Then the article will conclude with approachable proposals from the comparative analysis on how to strengthen the Croatian reopening approach so that genuine innocence claims are not blocked by overly restrictive gatekeeping process by the courts. These cases were carefully selected to capture the judicial reasoning when new scientific evidence is invoked and should be enough to illustrate the gatekeeping logic and the decisive factors without distracting the reader with repetitiveness.

2. THEORETICAL ASPECTS OF THE REOPENING OF THE CRIMINAL PROCEDURE

When it comes to the reopening of the criminal procedure based on new facts or new evidence, the most common hypothesis used is the notion of new evidence. Consequently, this aspect has been at the core of numerous jurisprudential reforms, aimed at explaining its meaning, alternatively enlarging or reducing the application perimeter of the reopening. Even today, and among the analyzed jurisdictions here, there is no academic, nor hermeneutical consensus deriving

² Primorac, D.; Soćanović, L.; Bozhinovski, A., *Correcting Miscarriages of Justice: Innocence Project Croatia*, in: *Forensic Science and Molecular Anthropology: Topics Selected from 12th ISABS Conference on Forensic and Anthropological Genetics*, BoD–Books on Demand, 2024, p. 83.

³ Bozhinovski, A., *Protection of the Rights of Wrongfully Convicted Persons in Croatia*, SPLITLAW, 2025, p. 253.

from the fact as to what is and how should new evidence be evaluated.⁴ the classical criminal law hypothesis recognizes 3 (three) types of new evidence: *noviter productae* (pre-existing evidence, never evaluated nor presented at the trial), *noviter repertae* (evidence that has emerged after the finality of the judgment) and *noviter cognitae* (elements that were gathered during the trial but not assessed by the judge). Even though classical legal theory recognizes 3 (three) kinds of the new evidence, Luparia argues that in the judicial practice only *noviter repertae* evidence is accepted by the courts, when motions for reopening of the procedure is being filed.⁵

As to why this is the case, Pituritti and Luparia further argue that it is due to owing to the traditional necessity of stability of the judicial decisions and of protection of the normative status quo related to criminal justice.⁶ However, it should be mentioned that as a result, the possibility to file a motion for reopening was and it is still narrow. What is relevant for this paper, is that many jurisdictions, in recent development have undergone somewhat a new change, on the correct assumption that as technology changes, there are many new and modern ways to perform a retesting of already presented evidence, and that should constitute a novum. Hence, the most recent orientation is one that allows admission in the reopening of any evidence that escaped the appreciation of the judges, therefore including in the notion of 'new' evidence all the three types of evidence described. Reopening of the procedure can be filed on many grounds, and this is evident in the comparative proceedings which more or less are the same everywhere: against false testimony, false expertise, official misconduct by the actors of the procedure (prosecutor, judge, police, etc), furthermore, new evidence, trial in absentia and after a judgment of the ECtHR or the Constitutional Court, where some infringement of a procedural right is detected.⁷

There is an interdependence between reopening of the criminal procedure and judicial error, and in order to file a motion for a reopening, the only precondition is finality of the judgment or *res iudicata*. This is an extraordinary legal remedy, and it is interdependent with the *res iudicata*. The aim of this remedy is to prove judicial error or *error facti*, i.e. that the court has promulgated a wrongful judgement, and request to be removed from legal traffic. The purpose is to reveal the judge's faulty evaluation of the facts contained in the final decision, thus leading to its reversal. Therefore, the universal hypothesis of this legal remedy is

⁴ Lupária, L.; Cagossi, M.; Pittiruti, M., *Miscarriages of justice in Italy*, in: *Murder, Wrongful Conviction and the Law*, Routledge, 2023, pp. 113–114.

⁵ *Ibid.*, pp. 114–115.

⁶ *Ibid.*, pp. 68-69.

⁷ Bozhinovski, *op. cit.* note 3, pp. 260-264.

to correct a substantial injustice of the ruling, that is to say an error in the reconstruction of the historical event, leading to an unjust overcoming of the presumption of innocence.⁸

However, there is a relationship of interdependence, as described by Luparia. On the one hand, the alleged error is a prerequisite for the request of reopening, while, on the other hand, the judicial error acquires legal significance only following its assessment through the reopening judgment.⁹ With this in mind, it can affirm that reopening represents a system security mechanism, capable of guaranteeing the individual's personal freedom, in cases where an antinomy between the definitive statement of guilt pronounced and the historical truth is ascertained. This is why laws on criminal procedure, almost everywhere envisage that this extraordinary legal remedy can be filed by the convicted person, their defense counsel, family, partners, and even public prosecutor. The idea is to not to correct a private injustice, but public injustice (having in mind that correcting injustice is a public interest). Therefore, only the error that emerges from new facts can justify the overcoming of a final judgment, thus avoiding that the review may turn into a fourth degree of judgment.¹⁰ When it comes to new scientific evidence, this type of evidence relies on newly developed and highly specialized scientific methods which of course in a course of time are gradually changing and evolving. Therefore in principle, that evolution can expand and already presented evidence with an older method, can be retested with a newly developed method and yield a different result. Of course, given how the procedural rules for reopening of the procedure are envisaged in European legislations, the harder cases are those where the applicant seeks a new analysis of material already collected at trial, using evaluations that were not conducted at the time. The hardship in this is observed through the reassessment of evidence already examined.

However, the most contested ground for reopening represent the introduction of new evidence, which is the object of analysis in this paper. Gathering new evidence is one side of the coin, and how it is defined in the law is another. In assessing new scientific evidence, American standards developed through the doctrines of *Frye* and *Daubert* cases which will be discussed below, are much more developed than the European standards which do not have a single doctrine on how to evaluate new scientific method applied to a case. An exception to this rule is the *Ghiro* case, from the jurisprudence of the Italian Supreme Court, which mirrors the *Frye* standards, and sets the precondition on admissibility of new scientific evidence.

⁸ Lupária et al., *op. cit.* note 4, pp. 120–123.

⁹ *Ibid.*, p. 125.

¹⁰ Nan, J.; Holvast, N.; Lestrade, S., *A European approach to reopening in criminal matters?*, *Erasmus L. Rev.*, 13, 2020, pp. 102-104.

However, to present the full picture, the analysis first outlines the American and European standards governing when a new scientific method may be treated as "new evidence" for reopening purposes. It then turns to the national rules and judicial tests in a selected group of European jurisdictions, mapping how each system defines new evidence and how courts assess theirs.

3. AMERICAN AND EUROPEAN STANDARDS ON ADMISSIBILITY OF NEW SCIENTIFIC EVIDENCE

New scientific evidence is accepted in the U.S. court system, through 2 (two) established available standards. The first standard is the *Frye standard* or the *Frye test* which originated from the case of *Frey v. the United States*.¹¹ The Second standard is the *Dauber Standard* which originates from the landmark Supreme Court decision of *Daubert v. Merrell Dow Pharmaceuticals, Inc.*¹² *Frye test* or *Frye Standard* is employed by the court to assess whether the methodology or the scientific principle which was employed in the analysis of the DNA material, upon which the opinion of the expert is based is *sufficiently established to have gained general acceptance in the particular field in which it belongs in the relevant scientific community*.¹³ In other words, whether the employed standard is scientifically accepted and substantiated. Similar to this is the *Daubert* test or standard, which assigns the role to the judge as a gatekeeper on new scientific method, and evidence. The judge has to determine whether the reasoning of the expert, or the employed methodology can be applied to the facts of the case. The focus here is on the methodology used, and not on the conclusions that they generate. In practical implementation of this standard, the courts have established the following factors as guideposts for judges to assess: (1) Whether a theory or technique employed in the analysis of the material can be tested, (2) Whether the theory or technique has been subjected to peer review and publication, (3) the known potential rate of error, (4) the existence and maintenance of standards controlling the technique's operation, (5) the degree of general acceptance within the relevant scientific community.¹⁴

¹¹ *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923), *United States Court of Appeals for the District of Columbia Circuit*.

¹² *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), *United States Supreme Court*.

¹³ *Primorac et al.*, *op. cit.* note 2, pp. 434-436

¹⁴ Federal Rules of Evidence, Committee Print No. 11, 118th Congress, 2nd Session, December 1, 2024, *U.S. House Committee on the Judiciary*, U.S. Government Publishing Office, Washington, 2025. Rule 702, 703, and 404

Bearing in mind the nature of the scientific evidence (in all forms), and how very persuasive it is in determining material truth, it therefore must be handled very carefully, otherwise it will become misleading and may lead to wrongful convictions. When it comes to such limited profiles, the Federal Rules of Evidence imply that the court must take into consideration whether the prejudicial effect of such evidence substantially outweighs its probative value. In other words, the court must determine whether the introduction of such evidence unfairly prejudices a defendant by misleading the jury.

The treatment of scientific evidence in the continental European jurisdictions is regulated on a national and supranational level. However, importantly on a supranational level, the ECtHR addresses related issues through the lens of Articles 8 and 6 of the European Convention of Human Rights (hereinafter ECHR), thereby unifying the standards for all countries. The major discrepancy with the U.S. approach is that new scientific evidence in Europe, is not filtered through a Daubert/ Frye style test, and instead, judges assess credibility within the fact-finding process by exercising the principle of free evaluation of evidence. Concerning the admissibility standards of a scientifically new method, the European Court of Human Rights (hereinafter ECtHR) has established three pronged test, called the *Marper test*¹⁵, to take into account when assessing admissibility: (1) Legality of the measure, and (2) Proportionality of the retention period of DNA materials, meaning for severe crimes, the retention period must be longer, and (3) Removal of the DNA samples from the national database.¹⁶ When handling this information, there are two main requirements for the national authorities: The interference of the measure should have some basis in domestic law or a member state; and the law must be clear, foreseeable, and adequately accessible. Deviation from this criterion will result in a breach of Article 8 of the European Convention on Human Rights.¹⁷ The most notable ruling, which consequently established the admissibility test is the *S. and Marper v. the United Kingdom*¹⁸ case concerning the police retention of DNA profiles of individuals arrested but not convicted. In this case, the Court criticized the UK's practice of nonselective and indefinite retention as a significant invasion of privacy, especially problematic for minors and those not convicted, potentially impacting

¹⁵ This test is concerning the ramification, collection and storage of DNA evidence, but courts are applying the test to new scientific evidence as well, once it emerges.

¹⁶ Primorac, D.; Božhinovski, A., *Correcting Miscarriages of Justice in Croatia: Accession and Time-Limited Retention of DNA Profiles in the Jurisprudence of the European Court of Human Rights, EU and Comparative Law Issues and Challenges Series (ECLIC)*, vol. 7, 2023, pp. 487–490.

¹⁷ *Ibid.*

¹⁸ *S. and Marper v. the United Kingdom*, Applications nos. 30562/04 and 30566/04, Judgment of 4 December 2008, *European Court of Human Rights*.

their societal reintegration and violating children's rights protections under international law.

A key observation is that the U.S. and European approaches address new scientific evidence through different control points. In the United States, admissibility is structured around formal gatekeeping standards regulated in the Frye and Daubert standards, and the Federal Rules of Evidence, with the judge filtering scientific evidence primarily by scrutinizing the methodology. This reflects how cautious the American judiciary is in evaluating forensic science, especially in borderline scenarios (such as partial DNA matches). In continental Europe, by contrast, scientific evidence is typically not prefiltered through an equivalent methodology-focused admissibility test; it is instead observed into the broader fact-finding framework under the principle of free evaluation of evidence, with reliability debates often occurring within the merits assessment rather than at an admissibility "gate. However, interestingly, at the supranational level, the ECtHR's jurisprudence provides a different concept of the interpretation of new scientific method in new evidence.

4. DIVERGENT CONCEPTS ON NEW EVIDENCE IN EUROPEAN JURISDICTIONS

To further understand how new evidence standard impacts the reopening of the criminal procedure, a brief overview of how selected European jurisdictions define and assess new evidence in the context of reopening of criminal proceedings is needed. In this segment, the paper will focus on: France, Germany, Italy, the Netherlands, and Belgium, selected as countries that underwent major reform in the area of extraordinary legal remedies and post-conviction proceedings in general and expanded their definitions on what constitutes a new evidence or novum. The purpose here is to provide a full doctrinal account of each national remedy, and map definitional choices, whether these systems interpret new evidence in an extensive or restrictive manner.

In the Netherlands, reopening in favor of the convicted (*herziening ten voordele van een gewezen verdachte*) is an extraordinary legal remedy available. Once the initial trial finishes with the judgement, the parties of the procedure can file an appeal before the Court of Appeal. In this process, the judges will review the entire case again and should they decide not to accept the appeal, the parties then have the right to appeal to the Supreme Court, which investigates whether there was a proper application of the Law, and does not review the actual case, like some sort

of third instance.¹⁹ After the Supreme Court, the next phase is to file an application to the ECtHR whether some right of the ECHR was infringed. As soon as the term to do so has expired, or as soon as the ECHR procedure rejected the complaint, a conviction is irrevocable. The only way a case can be revised again, is by filing a successful request for review (*herzieningsverzoek*) at the Supreme Court or *ex officio* by the procurator general of the Supreme Court.²⁰ As to what changes were introduced concerning new evidence or fact, the latest amendments of the Law on Criminal Procedure stipulate Article 457 et seq from the Dutch Code on Criminal Procedure, regulates the cases when such a request can be filed. The first case is *on the grounds that in various judgments or judgements which have become final or were rendered by default, convictions have been rendered which cannot be reconciled*. The second case is *on the basis of a judgment of the ECtHR, for violation of some right within the ECHR*. The third, and relevant to this paper, is *if there is a fact that was not known to the judge during the investigation at the hearing and that, either in itself or in connection with the evidence previously provided, does not seem to be compatible with the ruling, such that a serious suspicion arises that if this fact had been known, the investigation of the case would have led either to an acquittal of the former suspect, or to a dismissal of all prosecution, or to the inadmissibility of the Public Prosecution Service, or to the application of a less severe penal provision*.²¹ Noted from the definition, the word fact is used. This prompted the Supreme Court on occasion to make an exception to the requirement that the new forensic evidence was of a factual nature and broadened its scope. Furthermore, Nan and Holvast, argue that new forensic expertise is considered a new fact, because bearing in mind that most wrongful conviction cases were based on faulty forensic expertise.²²

Belgium on the other hand, reopening is envisaged in Article 443 of the Law on Criminal Procedure envisages 3 (three) grounds for reopening of the criminal procedure.²³ The first envisages that *two (or more) distinct convictions that find different defendants guilty of the same fact and that are irreconcilable, so that one of the convicted persons has to be innocent*.²⁴ the second is the *after a conviction*,

¹⁹ Geven, L.; van den Doel, K., *Miscarriages of justice in the Netherlands*, in: *Murder, Wrongful Conviction and the Law*, Routledge, 2023, pp. 58–59.

²⁰ *Ibid.*, pp. 59-60.

²¹ Wetboek van Strafvordering, Article 457(1)–(2).

²² Holvast, N.; Nan, J.; Lestrade, S., *Between legal certainty and doubt: The developments in the procedure to overturn wrongful convictions in the Netherlands*, *European Law Review*, 4, 2020. <https://doi.org/10.5553/ELR.000188>.

²³ Article 443, *Code of Criminal Procedure [Wetboek van Strafvordering (Code d'instruction criminelle)]*, in force 7 December 1808 (consolidated version, 20 November 2025), *Federale Overheidsdienst Justitie (JUSTEL)*, available at: https://www.ejustice.just.fgov.be/img_l/pdf/1808/11/17/1808111701M_N.pdf

²⁴ Belgian Code of Criminal Procedure, Article 443 (1) (a)

*a witness that was heard is convicted for false testimony concerning the defendant.*²⁵ The third and important for our analysis here is *an element that was unknown to the judge during the initial proceedings and impossible for the convicted person to demonstrate at that time and that, alone or combined with the evidence that was gathered before, seems incompatible with the conviction, thus creating a strong suspicion that, if the element had been known, it would have led to an acquittal, a discontinuance of the proceedings or the application of a less strict criminal provision.*²⁶ Though the legal reforms were inspired by the Dutch approach to redefine the definition of what constitutes new evidence, the Belgian approach changes the word fact or evidence, with the word element. Verhesschen and Fijnaut note further that adding the word element extended the definition, and now new witness statement can be taken as evidence, and if reliable, they can be contested in new trial. Also, they argued it that the previous definition that mentioned only new evidence or a new fact (new testimony, new expertise) was deemed to be narrow, and unusable.²⁷

France has been the most pioneering in redefining the concept of reopening of the procedure to the advantage of the convicted person. Verhesschen and Fijnaut note that similar to Belgium, the application for a reopening is only allowed for more serious crimes which under the Criminal Code are the first and the second category: felonies, and ordinary offences, or misdemeanors (Art. 111-1 Code pénal).²⁸ Under Article. 622 of the Law on Criminal Procedure in France, simple finding of guilt is sufficient to initiate the proceedings, so the imposition of a penalty is not required. Moreover, the reopening procedure concerns only criminal decisions that are final.²⁹ Concerning the grounds of *novum* the French legislator unified all the grounds into one. Article 622 (1) of Law on Criminal Procedure stipulated that *A reopening can be requested when, after convictions, a new fact or an element unknown to the court at the time of trial emerges, and is of such a nature as to establish the person's innocence or raise doubt about their guilt.*³⁰ Prerequisite is new fact or the unknown element must not have been known to the court during the original proceedings, but may have been known to the applicant.

²⁵ Belgian Code of Criminal Procedure, Article 443(1) (b)

²⁶ Belgian Code of Criminal Procedure, Article 443 (1) (c).

²⁷ Verhesschen, K.; Fijnaut, C., *Chosen Blindness or a Revelation of the Truth?: A New Procedure for Reopening in Belgium*, *Erasmus Law Review*, 13(4), 2020, pp. 13–21. <https://doi.org/10.5553/ELR.000183>

²⁸ Article 111 (1) Code pénal (LEGITEXT000006070719). (n.d.). République française (Légifrance). Accessible at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719

²⁹ Verhesschen, K.; Fijnaut, C., *Correcting wrongful convictions in France: Has the Act of 2014 opened the door to reopening?*, *Erasmus Law Review*, 13(4), 2020, pp. 22–23.

³⁰ Code de procédure pénale, Article 622 (1),

However, prerequisite for a reopening to happen is a new fact or any unknown element (new) must not have been known to the court during the original proceedings.³¹ However, briefly stating in this segment, that the reforms of the Law on Criminal Procedure, also established the new court (*Cour de révision et de réexamen*) or the reopening court specialized only for reopening cases and composed of total of eighteen judges.³² The reopening court consists of two commissions: The *Commission d'instruction* (Investigation Commission), responsible for filtering and assessing the admissibility of reopening requests, and *The formation de jugement* (Adjudication Commission) which is a commission which decides on the substance and merits of the case.

Italy, a jurisdiction which is very close to the Croatian legislation has valuable lessons on the treatment of the scientific evidence. However, first reopening of the criminal procedure for the benefit of the convicted is stipulated in Article 630 of the Italian Law on Criminal Procedure, which is an extraordinary appeal to annul a wrongful conviction, and extraordinary appeal for factual errors.³³ This Article stipulates that reopening of the criminal procedure on the benefit of the defendant is permissible on 5 (five) grounds. First *if the facts underlying the judgment or the criminal decree of conviction are incompatible with those established in another final criminal judgment issued by the ordinary court or by a special court*. Second *if the judgment or criminal decree of conviction has based its decision on a judgment issued by the civil or administrative court and subsequently revoked, if a decision has been taken on one of the preliminary issues provided for in Article 3 of the Law on Criminal Procedure*. Third, (relevant to this analysis), *if new evidence is found or discovered after conviction and, either independently or together with already assessed evidence, proves that the convicted person must be acquitted*. Fourth *if it is proven that the judgment of conviction has been delivered on the basis of or as a consequence of false documents or statements provided during the trial or of any other criminal act deemed an offence by the law*. This ground must be integrated with the previous or established jurisprudence. Fifth, *reopening is based on compliance with a final judgment of the European Court of Human Rights*³⁴ However, a major breakthrough was made about the admissibility of new scientific methods applied to previously collected evidence. The Court of

³¹ Tourret, A., & Fenech, G. (2013). *Rapport d'information n° 1598 sur la révision des condamnations pénales*. Assemblée nationale, XIV^e législature. <https://www.assemblee-nationale.fr/14/rap-info/i1598.asp>

³² Code de procédure pénale Article 623 (1) and 624(2)-(6).

³³ *Italian Code of Criminal Procedure [Codice di Procedura Penale]*, 1988, Arts. 3, 11, 127, 420-bis, 529, 530, 606, 625-bis, 629, 629-bis, 630, 632–634, 636–637, 640–641, 643, 648–649, 479, available at: <https://www.normattiva.it/uri-res/N2Ls?>

³⁴ Italian Code of Criminal Procedure, Article 630 (1)

Cassation in the Ghiri case³⁵ has developed criteria for assessing reopenings based on new scientific methods. In this case the court has accepted that the new scientific method can serve as a *novum* as it was not in existence during the trial. In this judgement the Court of Cassation introduced the 5 (five) indicators on assessing the novelty of the method: a) the novelty of the scientific method (the method must be new in nature), b) the scientific credibility and reliability of the method (the method must be approved by the scientific community and widely published; it must not be experimental), c) the method should be applied to previously assessed evidence, d) the results should be novel in order to establish whether they are suitable to determining a new sentence, and e) the new results, should be able to justify a different outcome.³⁶ These conclusions of the Court of Cassation mirror the *Frey* and *Daubert* standards established by SCOTUS in assessing new scientific evidence.

German experiences indicate a different approach. Concerning the reopening based on new evidence, the Law stipulates that *if new facts or evidence are presented which, alone or in conjunction with the evidence previously gathered, are capable of justifying the acquittal of the accused or, by applying a more lenient penal law, a lesser punishment or a substantially different decision regarding a measure of rehabilitation and security*³⁷. Defining what facts are in this definition, the position of the Federal Constitutional Court is that *facts shall be understood as existing, identifiable occurrences or circumstances which belong to the past or the present. Whether a fact is new or not shall be judged solely according to whether or not the court has already utilized it. Therefore, in principle new is everything which the court has not taken as a basis for forming its opinion, even if it could have taken such as a basis*.³⁸ According to the research done by Lindemann and Lienau, it must be taken into account though that criminal courts are not obliged to address every taking of evidence made in the main proceedings within the context of its grounds for the ruling, therefore, in the failure to mention a piece of evidence which is substantial with respect to the basis of facts for the decision, one may see an indication of a failure to take such into account.³⁹

³⁵ Court of Cassation, Sec. I, 8 March 2011, Ghiri, in *C.E.D. Cass.*, no. 249864.

³⁶ *Ibid.*

³⁷ Article 359., *German Code of Criminal Procedure [Strafprozessordnung (StPO)]*, Bundesministerium der Justiz and Bundesamt für Justiz, available at: https://www.gesetze-im-internet.de/stpo/_359.html

³⁸ BVerfG, Resolution of the 2nd Chamber of the Second Senate, 19 July 2002 – 2 BvR 18/02, 2 BvR 76/02, *StV*, 2003, p. 225.

³⁹ Lindemann, M.; Lienau, F., *Mechanisms for correcting judicial errors in Germany*, SSRN, 5 May 2021, pp. 77–78.

Obviously, the new evidence is defined differently. Some jurisdictions have expanded the scope and ground of new evidence, by introducing the word element, instead of fact. Others have merged all grounds into one, and others simply kept the narrow interpretation of new evidence or new facts. However, two positive practices can be taken from this analysis in regard to Croatia.

The first is the Belgian definition of what constitutes new evidence. the LCP defines it as an element that was unknown to the judge during the initial proceedings and impossible for the convicted person to demonstrate at that time and that, alone or combined with the evidence that was gathered before, seems incompatible with the conviction, thus creating a strong suspicion that, if the element had been known, it would have led to an acquittal, a discontinuance of the proceedings or the application of a less strict criminal provision. The second positive experience is the Italian interpretation in the Ghirelli case, of what is a new scientific method, and how the court should reapply that method on already presented evidence.

5. CROATIAN LEGAL FRAMEWORK AND PRACTICE

5.1. Legal Framework

The Croatian legislator provides two kinds of reopening: extraordinary (triggered only in the sentencing part, where the court failed to account former convictions of the defendant, without entering the merits of the case) and proper reopening (where there are circumstances that the court might have made a mistake in application of substantial law).⁴⁰ Further, reopening of the criminal procedure can be on the benefit of the convicted person, and to the detriment of the convicted person, which is also not topic of analysis in this paper.

Reopening of the criminal procedure for the benefit of the convicted person, stipulated in Article 501 of the Law.⁴¹ This procedure and the processes are regulated in Articles 501–508 and it is intended as a safety net against miscarriages of justice. There are in total 5(five) grounds for reopening of the criminal procedure, where the first 2 (two) grounds cover reopening due to official misconduct committed through false testimony of experts, interpreters, witnesses,

⁴⁰ Criminal Procedure Act [*Zakon o kaznenom postupku*], consolidated text, Narodne novine, nos. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 126/19, 130/20, 80/22, 36/24, 72/25, 30 April 2025, available at: <https://www.zakon.hr/z/174/zakon-o-kaznenom-postupku>

⁴¹ CPA, Article 501 (1)

prosecutors, judges, jury members, investigators, police and any other person affiliated with the criminal procedure. Garačić further notes that the new evidence must establish a causal relationship between the crime committed and the final judgment passed, to provide concrete evidence that the final judgment is a result of official misconduct.⁴² For these 2 (two) grounds, paragraph 2 of the Law stipulates that new evidence can be considered only a judgment rendered against the person who committed official misconduct (false expertise, false testimony, etc). No other evidence except for a judgment, which indicates high threshold at the off start.

Further, the 3rd (third) ground is reopening based on new evidence or *novum*. The full legal provision is: *if new facts or new evidence emerge, which on their own or in connection with the previous evidence can lead to an acquittal or a conviction under more lenient criminal law*. Legal commentators, Zlatarić and Damaška argue that if the facts or evidence were already raised or assessed during the original trial or in a prior, dismissed reopening request, they do not qualify as new. This is the current position of the judiciary as well, because the burden is on the applicant to plausibly show that the new material could have changed the outcome. If the request relies only on previously considered facts or evidence, the court will dismiss it.⁴³ However, this definition must be observed through comparative analysis in other countries. It can be deducted that the legislator followed the German definition and provided a high degree of trust into the *res iudicata*, as well as the threshold upon which new evidence is admitted. The last 4th (fourth) and 5th (fifth) ground are reopening of the procedure due to incompatibility between final convictions, and cases of continued offence. Also connected with sentencing, this provisions regulates new facts which are affecting the scope of the sentence.⁴⁴ In the 5th (fifth) ground, reopening of the procedure is allowed in the cases of final judgments by the Constitutional Court of Croatia as well as a final judgment from the ECtHR (the European reopening), and for both cases the deadline for submission is 30 days, starting from the finality of the judgment.

⁴² Garačić, A., *Prava i nepravna obnova kaznenog postupka*, Hrvatska pravna revija, Zagreb, 2005, p. 112, available at: https://www.vsrh.hr/CustomPages/Static/HRV/Files/AGaracic_Prava-i-nepravna-obnova-postupka_2005.pdf

⁴³ Zlatarić, B.; Damaška, M., *Rječnik krivičnog prava i postupka*, Informator, Zagreb, 1966, p. 191.

⁴⁴ Lasan, V. D., *Obnova kaznenog postupka de lege lata i analiza odluka Ustavnog suda Republike Hrvatske donesenih u povodu ustavnih tužbi nakon obnove kaznenih postupaka na osnovi konačne presude Europskog suda za ljudska prava*, Hrvatski ljetopis za kaznene znanosti i praksu, 25(2), 2018, pp. 171–172.

Article 504 – 508 regulate the procedure of the motion for reopening of the procedure, who may submit the motion (the parties and the defense counsel; the state attorney and the persons listed elsewhere in the Law). It also clarifies that such motion can be submitted if the accused was tried *in absentia*, and regardless of whether the convicted person is present. Additionally, it states that reopening may be sought even after the sentence has been served, and irrespective of limitation, amnesty, or pardon. This is similar to the American solution of *Coram Nobis*. Furthermore, Article 505 regulates that the motion is decided by a panel of judges, of the court that tried the case at first instance in the earlier proceedings.⁴⁵ The motion can be submitted without the required form, but it must be clear on which ground the reopening is based, and what new elements are proposed. Furthermore, if any of those elements are missing the court can invite the applicant to supplement the request within a set deadline. Additionally, and relevant to the procedure, it excludes the participation of the judge or the panel of judges, who promulgated the earlier judgment. Additionally, Article 506 regulates the initial screening of the motion, and fact checking stage. Rejection of the motion is always granted, should it were filed by an unauthorized person, the statutory conditions or the threshold for reopening is not met, or the alleged new facts in the motion, were already presented and incapable of reaching the threshold of new evidence justifying reopening, or the applicant failed to comply by providing the court with additional materials.⁴⁶

The path of the motion is relatively straightforward and clear. Once the convicted person files the motion for reopening of the criminal procedure pursuant to Article 503 (1) (3), to the court which tried the case at first instance (this court can be either municipality court or county court, depending which one of them promulgated the first decision), the court decides upon the motion in a panel of judges. It is decided in the same court which promulgated the decision, but a different new panel. Then this panel starts the screening phase of the motion, assessing admissibility and plausibility whether is sufficient to engage a reopening. In this stage the panel may promulgate 3 (three) decisions: *to dismiss it* (it will dismiss it if the legal grounds are not met, such as: no statutory convictions, unauthorized person, repetition of the same facts, evidence, or the applicant failed to provide the court with supplemental document), *to accept it* (this does not automatically mean a new trial). Acceptance here means that the court considers the motion credible for further consideration, Then the president of the panel (personally or through an investigative judge) verifies and evaluates the new facts in the motion and initiates an investigation to collect that evidence.

⁴⁵ CPA, Article 505 (1)

⁴⁶ CPA, Article 506 (1) - (2).

After all actions are completed it sends the case to the opposing party to provide an opinion, which must be submitted in a period of 8 (eight) days. After this the court promulgates a decision on whether to grant reopening and schedule a new trial or reject the motion.), to *reject it*. It will be rejected when the court considers that the new evidence is not sufficient to reach the threshold of *novum*. Against this decision for rejection of dismissal, the convicted person, or their defense counsel are eligible to file an appeal to the second instance court. If first instance was municipal court, the appeal would be lodged to the county court, as second instance. If the first instance was the county court, the appeal will be lodged to the High Criminal Court, who is authorized to decide upon appeals in cases of reopening of the procedure.⁴⁷

The Croatian legal framework is forward-looking, and provides available legal avenues, available to persons who wish to challenge the validity of the judgment and prove judicial error. However Several observations need to be placed on the current definition on new evidence and new facts, the Croatian definition lacks a word of *new element* which in practical reference, places the threshold very high to introduce a new evidence.

5.2. Case Analysis

In this segment two selected cases from the jurisprudence of the County Court of Split, and the High Criminal Court will be reviewed to illustrate how in different cases the court evaluate and accept new scientific evidence. Both cases are approved for reopening, and contain different interpretation.

In the jurisdiction of the County Court in Split, in this case, the court acting as an appellate court granted a reopening of the criminal procedure on the benefit of the defendant based on new evidence. The defendant was found guilty of the criminal offense of forgery of a document and sentenced to 2 (two) years in prison. The applicant filed a motion for reopening of the criminal procedure, based on new evidence, more specifically a new graphological expertise. The first instance court rejected this request stipulating that the evidence was already evaluated and it is not credible enough to cause exoneration. and the County Court accepted his request and order a reopening of the case. The second instance court further

⁴⁷ Conclusions adopted at the meeting of presiding judges and registry judges of the Criminal Division of the Supreme Court of the Republic of Croatia with the presiding judges of the High Criminal Court of the Republic of Croatia and the presidents of the Criminal Divisions of all county courts, held on 9 June 2022] (Su-IV-21/2022-11), accessible at: www.vsrh.hr/EasyEdit/UserFiles/zakljucci-ko/2022/su-iv-21-2022-11.pdf

stipulated that during the proceedings before the first instance court, witnesses were examined, including SMS correspondence between the convict and the witness and based on these evidence, and without graphological examination, the applicant was found guilty of committing the criminal offence of forgery of a document. However, the second instance court, has established that in the new evidence, submitted as part of the motion (new expert opinion), contained graphology examination of the signature of the applicant, using a new developed method which was not in existence during the first trial. The new expertise concluded that the signature of the applicant on the purchase and sale contract for the motor vehicle almost certainly did not belong to the applicant. Therefore the aforementioned expertise points out that this new fact is appropriate to lead to an acquittal, especially since the convict was finally convicted without conducting a graphological expertise in the first trial⁴⁸

The second case answers the question, what if the new evidence is a new technique which was not existent at the time of the trial? Would that be counted as new evidence or not? Such was the decision of the Supreme Court allowing reopening of the procedure based on new evidence to take place based on new expertise. The County Court of Bjelovar as first instance court in this case, has rejected the motion of the applicant for reopening of the criminal procedure based on new evidence, claiming that the supplementary expertise did not indicate new evidence, rather provided just an interpretation of the evidence which was presented in the original trial. However, the Supreme Court appraised the situation, and decided differently, upheld the appeal from the applicant and ordered the court to take additional investigatory actions, based on the presented new evidence, and to test them in a new trial. The case revolves around attempted robbery, and the applicant was sentenced to 3 (three) years in prison. He filed a motion for reopening, based on new evidence, which in this case was a supplementary expertise, a forensic 3D reconstruction and biometrical analysis conducted by a registered expert, which concluded that due to a significant height difference of the applicant (14.8 to 17 cm), the applicant could not have been one of the masked perpetrators captured on the security camera footage of the crime, as he was taller than them. The new scientific method presented used a new version of photogrammetric software and the latest laser 3D scanner, which was not used in practice during the first trial (before 2009). However, in evaluating what new evidence represents, the Supreme Court found the decision of the first instance court to be premature and failed to take into consideration the fact that such technology had not existed during the first trial. The court reasoned that the new

⁴⁸ County Court in Split [Županijski sud u Splitu], Decision [Odluka], Kž-200/2022-5, 2022.

expert analysis, which used technology not available at the time of the original trial, presented potential new facts that could indeed impact on the factual basis of the conviction. Therefore, instead of dismissing it, the first instance court was instructed to send the request to the opposing party for a response, conduct an inquiry to verify the facts, and only then make a decision on whether to allow or deny the reopening.⁴⁹ Another interesting point raised in this case, was that the second instance court stipulated that the *judge cannot place himself in a role of a court expert*, although it does not possess the expert knowledge to assess the reliability of the forensic 3D reconstruction using laser 3D scanning of the crime scene.

These cases illustrate patterns of changed behavior of the judicial position concerning interpretation of new evidence or new facts when new forensic techniques are used to reevaluate evidence which was previously presented. This is an approach in a positive direction, and it is in line with the Italian standards established in the Ghiri case. Although Ghiri was evaluating newly presented scientific evidence, and established the admissibility criteria for forensic DNA evidence, such practice was not detected during the analysis of the judicial practice. However, the following case demonstrates the position of the Supreme Court in terms of new scientific evidence when DNA evidence is in question. However, no unified position exist on how to evaluate new evidence, especially scientific evidence, using the Ghiri method.

6. CONCLUSION

As mentioned in the prior text, the grounds for the possibility of filing a motion for reopening was and it is still narrow. What is relevant for this paper, is that many jurisdictions, in recent developments have undergone a new change, on the correct assumption that as technology changes, there are many new and modern ways to perform a retesting of already presented evidence, and that should constitute a *novum*. Therefore, changes in the Croatian definitions and the method of interpretation of new evidence need to be made.

Reopening of the procedure can be filed on many grounds, and this is evident in the comparative proceedings which more or less are the same everywhere: against false testimony, false expertise, official misconduct by the actors of the procedure (prosecutor, judge, police, etc), furthermore, new evidence, trial in absentia and

⁴⁹ Supreme Court of the Republic of Croatia [Vrhovni sud Republike Hrvatske], Judgment [Presuda], I Kž-153/2018-4, Zagreb, 2018.

after a judgment of the ECtHR or the Constitutional Court, where some infringement of a procedural right is detected. There are different definitions of *novum*, some countries are more explicit, other less, but the Belgian solution would be more approachable and applicable. The reason for that is because it contains the word *element* instead of facts. New element in this context, does not explicitly related to a new fact. Element is broader term, and can capture new expert development, or scientific reevaluation, a new witness coming forward, or a new digital trace. Furthermore, the definition stipulates that this element must have been unknown to the judge. the focus here is on what the court did not know, not on whether the court case technically contained something. That helps when the problem was misinterpretation or when the relevance of a piece of information only becomes clear later. Further, the definition captures the moment impossible for the convicted person to demonstrate at that time. This is based on protection of the wrongfully convicted as it covers few logistical problems such as: no access to forensic testing, no financial resources, or no legal aid. Finally, the definition contains the conjunctive and states that this element alone or combined with the evidence already gathered. This wording obligates the court to reassess the impact and strength of this element, and determine does this change the overall evidentiary picture. Furthermore, the lessons from the Italian jurisprudence need to be taken as an example. In this judgement the Court introduced the 5 (five) indicators on assessing the novelty of the method: a) the novelty of the scientific method (the method must be new in nature), b) the scientific credibility and reliability of the method (the method must be approved by the scientific community and widely published; it must not be experimental, c) the method should be applied to previously assessed evidence, d) the results should be novel to establish whether they are suitable to determining a new sentence and e) the new results, should be able to justify a different outcome.

In Croatia, reopening of the criminal procedure should be a subject of several changes. First, as seen from the comparative experiences, adding *new element* to this definition will lower the threshold for admissibility of new evidence. Furthermore, this definition does not contain the word *unknown to the court during the trial*, as in other jurisdictions analyzed where it is explicitly mentioned that the new element, new facts or new evidence, were not known to the court during the trial. This can lead to reading new evidence and new facts, very strictly and in further application, it may lead to inconsistencies in the interpretation of the same evidence. In practice, usually this is new forensic or scientific expertise. However, doctrinally this formulation needs to be amended and made more precise, to include new element, and add the wording unknown to the court during the first trial.

Another point here would be to provide whether additional clarification needed in the current phrasing can lead to acquittal or application to more lenient law. As such this is quite a strict threshold, and requires trial before a trial. The wording should not be that determinative especially during the initial screening of the request, because the applicant should not have to prove his/her innocence upfront but should cast a doubt that the evidence he/she is suggesting creates serious doubt about the correctness of the conviction or a realistic possibility of a different outcome. That is what the reopening of the trial is for, to determine the facts.

Another amendment is recommended in the process of deciding whether to accept, dismiss or reject the motion for reopening of the procedure. In the analyzed cases, the Supreme Court suggested that judges are not experts, and because they do not possess the relevant expertise, it would be premature for them to decide whether a new expertise is technically credible or not. They should only focus on admissibility. Therefore, this gatekeeping phase, needs to be a subject for thorough review.

REFERENCES

BOOKS AND ARTICLES

1. Bozhinovski, A., *Protection of the Rights of Wrongfully Convicted Persons in Croatia*, SPLITLAW, 2025. p. 253 – 264.
2. Garačić, A., *Prava i neprava obnova kaznenog postupka*, Hrvatska pravna revija, Zagreb, 2005., pp. 108-119.
3. Holvast, N.; Nan, J.; Lestrade, S., *Between legal certainty and doubt: The developments in the procedure to overturn wrongful convictions in the Netherlands*, *European Law Review*, 4, 2020., pp. 1-11.
4. Lasan, V. D., *Obnova kaznenog postupka de lege lata i analiza odluka Ustavnog suda Republike Hrvatske donesenih u povodu ustavnih tužbi nakon obnove kaznenih postupaka na osnovi konačne presude Europskog suda za ljudska prava*, *Hrvatski ljetopis za kaznene znanosti i praksu*, 25(2), 2018., pp. 169-196.
5. Lindemann, M.; Lienau, F., *Mechanisms for correcting judicial errors in Germany*, SSRN, 5 May 2021., pp. 73-86.
6. Lupária, L.; Cagossi, M.; Pittiruti, M., *Miscarriages of justice in Italy*, in: *Murder, Wrongful Conviction and the Law*, Routledge, 2023. 103–121.
7. Nan, J.; Holvast, N.; Lestrade, S., *A European approach to reopening in criminal matters?*, *Erasmus L. Rev.*, 13, 2020., pp. 102-109.

8. Primorac, D.; Božinovski, A., *Correcting Miscarriages of Justice in Croatia: Accession and Time-Limited Retention of DNA Profiles in the Jurisprudence of the European Court of Human Rights, EU and Comparative Law Issues and Challenges Series (ECLIC)*, vol. 7, 2023., pp.477-501.
9. Primorac, D.; Soćanović, L.; Bozhinovski, A., *Correcting Miscarriages of Justice: Innocence Project Croatia*, in: *Forensic Science and Molecular Anthropology: Topics Selected from 12th ISABS Conference on Forensic and Anthropological Genetics*, BoD–Books on Demand, 2024. p. 83-101.
10. Verhesschen, K.; Fijnaut, C., *Chosen Blindness or a Revelation of the Truth?: A New Procedure for Reopening in Belgium*, *Erasmus Law Review*, 13(4), 2020., pp. 1-14.
11. Verhesschen, K.; Fijnaut, C., *Correcting wrongful convictions in France: Has the Act of 2014 opened the door to reopening?*, *Erasmus Law Review*, 13(4), 2020., pp. 22-32.
12. Zlatarić, B.; Damaška, M., *Rječnik krivičnog prava i postupka*, Informator, Zagreb, 1966, p. 191.

LEGAL ACTS

1. *Code of Criminal Procedure [Wetboek van Strafvordering (Code d'instruction criminelle)]*, in force 7 December 1808 (consolidated version, 20 November 2025), *Federale Overheidsdienst Justitie (JUSTEL)*
2. *Criminal Procedure Act [Zakon o kaznenom postupku]*, consolidated text, Narodne novine, nos. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 126/19, 130/20, 80/22, 36/24, 72/25, 30 April 2025.
3. Federal Rules of Evidence, Committee Print No. 11, 118th Congress, 2nd Session, December 1, 2024, *U.S. House Committee on the Judiciary*, U.S. Government Publishing Office, Washington, 2025.
4. *German Code of Criminal Procedure [Strafprozessordnung (StPO)]*, Bundesministerium der Justiz und Bundesamt für Justiz.
5. *Italian Code of Criminal Procedure [Codice di Procedura Penale]*, 1988,
6. Turret, A., & Fenech, G. (2013). *Rapport d'information n° 1598 sur la révision des condamnations pénales*. Assemblée nationale, XIVe législature., pp. 1-115.

COURT PRACTICE

1. Conclusions adopted at the meeting of presiding judges and registry judges of the Criminal Division of the Supreme Court of the Republic of Croatia with the presiding judges of the High Criminal Court of the Republic of Croatia and the presidents of the Criminal Divisions of all county courts, held on 9 June 2022] (Su-IV-21/2022-11), accessible at: www.vsrh.hr/EasyEdit/UserFiles/zakljucci-ko/2022/su-iv-21-2022-11.pdf?
2. County Court in Split [Županijski sud u Splitu], Decision [Odluka], Kž-200/2022-5, 2022.
3. Italian Court of Cassation, Section I, 8 March 2011, No. 15139, Ghio, in CED Cass., No. 249864.
4. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), *United States Supreme Court*
5. *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923), *United States Court of Appeals for the District of Columbia Circuit*.
6. German Federal Constitutional Court [BverfG], Resolution of the 2nd Chamber of the Second Senate, 19 July 2002 – 2 BvR 18/02, 2 BvR 76/02, *StV*, 2003, p. 225.
7. *S. and Marper v. the United Kingdom*, Applications nos. 30562/04 and 30566/04, Judgment of 4 December 2008, *European Court of Human Rights*.
8. Supreme Court of the Republic of Croatia [Vrhovni sud Republike Hrvatske], Judgment [Presuda], I Kž-153/2018-4, Zagreb, 2018.

UDK: 336.7 (439) 343.359 (439)
Professional paper

Tamás Károly Goricsán, PhD student
Faculty of Law, University of Pécs, Hungary
E-mail: goricsan.tamas@ajk.pte.hu
ORCID-ID: 0009-0004-1795-0771

THOUGHTS ON THE EFFECTIVENESS OF MEASURES AGAINST MONEY LAUNDERING

ABSTRACT

Hungary adopted, in Government Decision No. 1688/2017 (IX. 22.), an action plan for implementing the anti-money laundering recommendations made by the Moneyval. Based on Moneyval's fifth-round country report, Hungary was required to make appropriate progress in the areas of practical implementation and effective task performance. Furthermore, Act XLIII of 2020, amending the Criminal Procedure Act, redefined the money laundering as of 1 January 2021 in order to comply with Directive (EU) 2018/1673 of the European Parliament and of the Council. One of the typical forms of money laundering is committed by the so called financial agents. In many instances, the predicate offense is committed abroad, or the funds are transferred abroad from Hungarian transit accounts, thus necessitating cross-border criminal cooperation, evidence can generally be obtained only through judicial cooperation mechanisms. Eurojust serves as a forum for judicial cooperation, which investigating authorities can access through the public prosecutor's office. The International Law Enforcement Cooperation Center, operating within the National Police Headquarters, provides additional channels for police cooperation through Europol and Interpol. Data and information may also be obtained informally from foreign partner agencies, however, a formal request for legal assistance should not be omitted, even in such cases. Where a money laundering account is held at a foreign financial institution, an urgent request must be sent to National Tax and Customs Administration to contact the foreign partner and request the suspension of transaction. Accordingly, effective action against international money laundering is inconceivable without the exchange of cross-border information and data.

Keywords: money laundering, judicial cooperation, cross-border data exchange.

1. INTRODUCTION

Money laundering is a crime in which income obtained through criminal means is "cleaned" by returning it to the legal economy through secret, seemingly legal financial transactions. With the globalization of financial markets and the development of information technology, organized crime groups are increasingly able to hide illegal income and invest it in the financial sector.¹ Although money laundering does not have victims in the traditional sense, it has serious long-term consequences: laundered money sustains and finances organized crime and other serious crimes, while also fueling corruption and even terrorism financing in hidden ways. However, laundered illegal money does not only strengthen criminal circles.

Money derived from criminal activities undermines the integrity of financial systems and seriously jeopardizes public confidence. Money laundering distorts market competition, giving an advantage to economic actors who use illegal funds, while putting honest businesses at a disadvantage. This is harmful from an economic perspective, as the presence of fictitious capital can lead to a slowdown in economic growth and financial instability in the long term.

The fight against money laundering is a fundamental element of international law. The nature of money laundering is a crime relationship, and prosecuting perpetrators provides law enforcement with an effective tool in its fight against the predicate offenses, both in terms of detecting them and preventing the proceeds from being reused for criminal purposes.² Hungary is a signatory to the guidelines of the United Nations and the Financial Action Task Force³ (FATF) and is therefore obliged to implement the relevant conventions and recommendations. In addition, as a member state of the European Union, it is obliged to transpose EU anti-money

¹ Pintér, B., *A pénzmosás elleni küzdelem az új magyar büntető törvénykönyvben (Combating Money Laundering in the New Hungarian Criminal Law)*, doktori értekezés (doctoral thesis), Pécsi Tudományegyetem, Pécs 2012, p. 2.

² Belovics, E.; Molnár, G.; Sinku, P., *Büntetőjog II, Különös Rész (Criminal Law II, Special Part)*, ed.: Belovics, E., HVG-ORAC, Budapest 2021, p. 827.

³ The Financial Action Task Force is an intergovernmental organization that sets international standards for combating money laundering and terrorist financing. In order to protect the financial system from the risks of money laundering and terrorist financing and to ensure more effective compliance with international counter-terrorism strategies, the FATF identifies countries that have strategic deficiencies in their AML/CFT regimes. The organization calls on these countries to develop action plans and eliminate the identified deficiencies within a specified time frame. Financial Action Task Force, international standards on combating money laundering and terrorist financing, Hungarian National Bank website, <https://www.mnb.hu/felugyelet/szabalyozas/penzmosas-ellen/korlatozo-intezkedesek-szankciok/penzugyi-akciocsoport-fatf>, 14 January 2026.

laundrying directives and regulations. In recent years, the EU has adopted a new regulatory package in the area of money laundrying and terrorist financing: In May 2024, the European Council approved new regulations that establish a European Anti-Money Laundrying and Counter-Terrorist Financing Authority and harmonize and tighten anti-money laundrying rules. The new regulations extend the scope of obligated financial and non-financial service providers, tighten the registration of beneficial owners and restrictions on the use of cash, and clarify the list of high-risk third countries.⁴ All this shows that the fight is becoming increasingly stringent within the EU framework and that cooperation between national institutions is deepening. In Hungary, the most important framework regulation is Act LIII of 2017 on the prevention and combating of money laundrying and terrorist financing.⁵ Hungarian legislation applies an international risk-based approach, which means that the risks of money laundrying and terrorist financing must be regularly assessed and identified. Since 2017, Hungary has been regularly preparing its national risk assessment, which outlines the greatest risks of money laundrying. Within the national institutional system, the Office for Combating Money Laundrying and Terrorist Financing (as the Financial Intelligence Unit, operating within the National Tax and Customs Administration, hereinafter: NTCA FIU) collects and analyzes reports of suspected money laundrying and forwards the data to competent law enforcement agencies.

The Hungarian National Bank and other specialized authorities supervise financial and investment service providers, while professional chambers monitor the customer due diligence obligations of non-financial professions (e.g., lawyers, auditors). The AML/CFT Act is therefore based on complex cooperation: financial sector players are required to analyze and report risks, supervisory authorities monitor compliance with regulations, and the judiciary enforces the rules through law enforcement activities.

In Hungary, the number of money laundrying crimes⁶ detected and registered in police proceedings has increased significantly in recent years. While the number

⁴ Information Note for Members of Parliament, Office of the Hungarian National Assembly, Public Collections and Public Education Directorate, Representative Information Service, No. 2025/18, 30 May 2025.

⁵ 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról (on the prevention and combating of money laundrying and terrorist financing), Magyar Közlöny 2017/75., (hereinafter: AML/CFT Act).

⁶ This article does not aim to provide a detailed description of the current legal framework governing money laundrying. For more details: Gál, I. L., *Dogmatikai problémák a pénzmosás hatályos magyar szabályozásával kapcsolatban (Dogmatic problems related to the current Hungarian regulations on money laundrying)*, Belügyi Szemle, 71. évfolyam, 2023/5., pp. 741–763.

of money laundering offenses registered in the Unified Investigative Authority and Prosecutor's Office Criminal Statistics System was only 299 in 2020, this number reached 1,154 in 2024 and then 882 in the first seven months of 2025 (which predicted that the number of registered money laundering cases could exceed 1,500). However, the reasons for this increase are not only found in the proportional increase in the number of crimes (which is true, as the number of frauds committed online, which constitute the predicate offense of money laundering, and frauds committed using information systems has indeed increased⁷), but also to certain measures implemented to improve detection.

This professional article analyses this developments, with particular emphasis on the interaction between legislative reform and enforcement practice. The methodology of this study is descriptive and analytical; due to space constraints, I have not attempted to provide a critical, scholarly analysis of anti-money laundering measures. My primary focus here was on presenting the key legislative and other relevant measures that have made the fight against money laundering in Hungary faster, more effective, and thus more efficient for law enforcement agencies, while also providing an opportunity to learn about best practices and methods at the international level.

2. MAIN INSTITUTIONAL AND LEGISLATIVE MEASURES ENHANCING EFFECTIVENESS

2.1. Adopting the action plan against money laundering

Following the 5th round evaluation, the Hungarian Government adopted an action plan⁸ for implementing the recommendations made to Hungary by the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (hereinafter: Moneyval). Based on the Moneyval 5th round country report, Hungary had to make appropriate progress primarily in the areas of practical implementation and effective task performance, to comply with this, the action plan defined tasks for the competent authorities⁹.

⁷ According to Unified Investigative Authority and Prosecutor's Office Crime Statistics, for example, the number of online fraud offences registered between 2021 and 2022 in police proceedings nearly doubled (from 6,344 to 11,389).

⁸ 1688/2017. (IX. 22.) Korm. határozat az Európa Tanács Moneyval országjelentésben Magyarország részére megfogalmazott pénzmosás elleni ajánlások végrehajtásáról készített akciótervről (Government Resolution on the action plan for implementing the recommendations against money laundering made to Hungary by the Moneyval), Magyar Közlöny 2017/153.

⁹ In addition, the Hungarian Government also adopted 1691/2018. (XII. 17.) Korm. határozat a pénzmosás és terrorizmus finanszírozása elleni nemzeti kockázátértékelés

The tasks assigned to the National Police Headquarters in the action plan included, among other things,¹⁰ the preparation of a methodological guide for investigative authorities, which would facilitate, on the one hand, the development of a uniform law enforcement practice for investigations initiated on suspicion of money laundering, and, on the other hand, to enable the separation of cases involving predicate offenses and money laundering, as well as the continuation of money laundering investigations even after the investigation of the predicate offense has been completed. In addition, it helps investigative authorities to focus on the highest risks, in line with the findings of the National Risk Assessment, and assists in the investigation of the most serious and sophisticated cases of organized money laundering.

This methodological guide¹¹ stipulates that the condition for establishing money laundering is a punishable predicate offense, which must be established at least at the level of simple suspicion.¹² Unlike the legal regulations of some other countries, Hungarian criminal law does not recognize the category of autonomous money laundering, i.e., when unusual transactions without any underlying crime can also be classified as money laundering.¹³

In this regard, data is needed to prove that the property originates from a punishable offense¹⁴ that is contrary to the specific provisions of the Hungarian

felülvizsgálata eredményeképp megfogalmazott intézkedésekről (Government Resolution on measures adopted following the review of the national risk assessment for money laundering and terrorist financing), Magyar Közlöny 2018/201.

¹⁰ The action plan against money laundering also called for increasing the capacity of the National Bureau of Investigation of the Riot Police, setting up an operational committee with the participation of law enforcement agencies involved in anti-money laundering, the organization of joint investigation teams, the review of legal practice, and the organization of multidisciplinary expert consultations and training.

¹¹ The author of this paper contributed significantly to the preparation of this methodological guide, as well as the methodological guide referred to later, which was initiated due to suspicions of social engineering fraud and the development of a uniform practice for investigating internet-based property crimes, and to support the specialized investigation of specific types of fraud.

¹² In Hungarian Supreme Court decision No. BH 2019.125, the court ruled that in the case of the predicate offense and money laundering, a genuine heterogeneous formal combination cannot be created, i.e., a single act cannot simultaneously fulfill the legal elements of the predicate offense and money laundering.

¹³ Gál, I. L., ed., *Magyar büntetőjog, Különös Rész (Hungarian Criminal Law, Special Part)*, Osiris, Budapest 2023, p. 511.

¹⁴ A criminal offense and a punishable offense are not synonymous. The commission of a criminal offense is an essential condition for the imposition of a penalty. Since the law uses the concept of a punishable offense (disposition-like offense), money laundering can be established even if the perpetrator's act is only disposition-like, but the perpetrator cannot

Criminal Code¹⁵; it can be e.g. a report by a financial service provider of an unusual transaction suspected of money laundering, a report by the victim, a report or message from a bank, a report by the NTCA FIU, a report by a foreign authority in connection with its own proceedings within the framework of international criminal cooperation, on the basis of which there is a simple suspicion of a criminal offense. The basic facts must therefore be proven to some extent in proceedings for money laundering. It is not sufficient to make assumptions or probabilistic inferences based on reports, it must be proven that the money actually derives from a punishable offense.¹⁶

In this context, it is necessary to emphasize that if, as a result of its evaluation and analysis activities, NTCA FIU provides the investigating authority with basic information on suspicious transactions and the use of straw men, on the basis of which a suspicion of money laundering can be established, an investigation (or, where justified, a supplementary report) must be ordered.¹⁷ Nowadays, an increasing proportion of crimes are committed using computers and the internet, and computers can also be a source of evidence. When defining crimes against property committed in cyberspace, it is necessary to consider which crimes fall within the narrower definition of crimes against property. In practice, two crimes from Chapter XXXVI of ACC fall into this category: fraud and fraud committed using an information system.¹⁸

According to Section 3(1)(d) of Credit Institutions Act¹⁹, the provision of payment services qualifies as a financial service. Pursuant to Section 6(1)(87), all activities necessary for payment and bank account management are considered payment services. According to Section 2(8) of Payment Services Act²⁰, an account opened

be punished for some reason, in Földvári, J.; Gál, I. L., *Magyar büntetőjog, Általános Rész (Hungarian Criminal Law, General Part)*, Osiris, Budapest 2024, p. 316.

¹⁵ 2012. évi C. törvény a Büntető Törvénykönyvről (Act on the Criminal Code), Magyar Közlöny 2012/92. sz., (hereinafter: ACC).

¹⁶ Gál, *op. cit.* note 13, p. 511.

¹⁷ A 2017. évi XC. törvény büntetőeljárásról (Act on the Criminal Procedure), Magyar Közlöny 2017/99. sz., (hereinafter: ACP) Part Nine provides for the possibility of initiating preparatory proceedings within the framework of criminal proceedings.

¹⁸ Separate criminalisation of damage caused using information systems in Hungarian criminal law, conceptual distinction from traditional fraud; however, it is necessary to regulate this conduct separately from fraud, as it does not involve misleading or deceiving others in the traditional sense. The damage is caused by the unlawful influence of the information system. Accordingly, the law regulates fraud committed using information systems as a separate offense in the chapter on crimes against property.

¹⁹ 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (Act on Credit Institutions and Financial Enterprises), Magyar Közlöny 2013/217.

²⁰ 2009. évi LXXXV. törvény a pénzforgalmi szolgáltatás nyújtásáról (Act on the provision of payment services), Magyar Közlöny 2009/100. sz.

in the name of one or more customers of a payment service provider for the purpose of executing payment transactions is considered a payment account, including a bank account.

In the case of money laundering [Section 399(2) and (3) of the ACC], the use of financial services constitutes a criminal offense only if it is related to property derived from the commission of a punishable act. Opening a bank account creates the possibility of subsequent financial transactions involving assets derived from the underlying act. Therefore, opening an account is generally not sufficient to establish criminal conduct, but a bank account opened in Hungary may, depending on the results of the investigation, prove the existence of an agreement concluded in Hungary for bank transactions involving sums derived from the commission of a punishable offense, and thus also the account holder's intention to cooperate in the predicate offense or in the related money laundering offense. The opening of an account in Hungary to be used for subsequent money laundering may therefore, even in the absence of conduct that can be assessed as criminal behavior, give rise to suspicion of preparation for money laundering in violation of Section 399(8) of the ACC and may constitute grounds for jurisdiction.

In addition to the above, depending on the outcome of the evidence, opening a bank account may also constitute aiding and abetting the predicate offense. The opening of a bank account or making it available may also be a prerequisite for the fraudulent, damaging basic act; without it, the victim's bank account could not be debited, so it must be examined whether the account holder was aware of the precise scope of the act; whether they understood the necessary connection between the damage caused as a result of the victim's deception and the making available of the bank account.

2.2. Relevant legal amendments

In the interests of effective action, Act XLIII of 2020 amending the CPA²¹ re-regulated the legal definition of money laundering as of January 1, 2021, in order to comply with 6AMLD.²² The new definition continues to punish all conduct that was punishable under the previous definition, but for clarity, it recodifies the individual basic cases in separate paragraphs without changing their systemic

²¹ 2020. évi XLIII. törvény a büntetőeljárásról szóló törvény és más kapcsolódó törvények módosításáról (amending the Criminal Procedure Act and other related acts), Magyar Közlöny 2020/129.

²² Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284 of 12/11/2018.

significance. The amended provision aims to more effectively enforce the original criminal policy objective of criminalization, according to which crime can be more effectively curbed by preventing the financial gains from crime.²³ The most significant amendments are as follows:

- the range of money laundering offenses that can be committed by the perpetrator of the predicate offense has been expanded, as the material and intentional predicate offense of dynamic money laundering [Section 399 (1) and (2)] of the ACC no longer require the predicate offense to be committed by another person;²⁴
- more differentiated legal consequences are applied with the introduction of a system for classifying the value of the offense;
- instead of the object of the offense defined as a thing, the concept of property is used, which is not defined in either the ACC or the ACP;
- in dynamic basic cases [Section 399 (1) and (2) of the ACC], concealment is replaced by a new behavior, namely covering up, but this does not represent a substantive change;
- in the case of intentional dynamic money laundering [Section 399(2) of the ACC], the new conduct is receiving, using, concealing, disposing of, or participating in the alienation of property. In the case of self-laundering, these are distinguished from non-punishable subsequent acts by their intent. According to the detailed explanatory memorandum to the law, the common feature of these punishable acts is that, due to the fraudulent conduct associated with them, they go beyond the intended use of the property and cause additional damage;
- it highlights measures aimed at asset recovery and confiscation from the range of legal consequences for the perpetrator of the basic offense in cases of aiding and abetting [Section 399(3) of the ACC], while attempts to thwart other measures taken by the authorities in criminal proceedings are protected under criminal law through other legal provisions. This conclusion can only be reached if the criminal conduct is expressly aimed at avoiding the legal consequences related to the property;
- the basic case of aiding and abetting [Section 399(3) of the ACC] may also be committed by the perpetrator of the predicate offense, but only as a perpetrator [Section 399(9) of the ACC];
- the amendment repealed the offense of receiving stolen goods and integrated its criminal conduct into the basic case of static money laundering [Section 399(4) of the ACC]. In addition, the legislator

²³ Belovics; Molnár; Sinku, *op. cit.* note 2, p. 827.

²⁴ We speak of dynamic money laundering when the vast majority of criminal activities result in wealth transformation, whereas in the case of static money laundering, there is no such wealth transformation in economic terms, in Gál, *op. cit.* note 13, p. 512.

supplemented the acts constituting the basic case of static money laundering, adding a new element, namely the acquisition of the right of disposal, which is the contractual equivalent of the acquisition of property. The perpetrator of the predicate offense is not liable for this change either;

- all preparatory acts – not just the agreement to commit the offense jointly – are punishable [Section 399(8) of the ACC].

2.3. Other regulations relating to criminal proceedings

With regard to money laundering cases, the Department of Priority and Military Cases of the Hungarian Prosecutor General's Office issued Circular No. KF.9725/2004/379-II.²⁵ According to the circular, during the investigation, it is also a primary consideration that, in addition to measures taken to secure assets, all asset-generating (economic, or property) activities must be investigated to determine whether, after the completion of the predicate offense, the perpetrator of the predicate offense or another person committed any further acts in connection with the illegally acquired property that constitute money laundering in any form. If so, the investigation must be extended to include the crime of money laundering. One of the typical types of money laundering cases uncovered is money laundering committed by so-called financial agents. In these cases, the perpetrators typically agree with persons who remain unknown to open bank accounts or make their existing accounts available, with the understanding that they will transfer the money received in the account in exchange for an "agency fee" or withdraw it in cash and hand it over to an unknown person, or transfer it to a third country via money transfer services.

The perpetrator's state of mind can only be assessed based on all the evidence. Bank transactions carried out on behalf of and on the instructions of the principal in a bank account opened for someone else in the hope of receiving a commission conceal the identity of the person who actually controls the money, while the withdrawal of cash from the proceeds of the predicate offense serves to make it impossible to trace the assets, i.e., to conceal and hide the location of the money. It should be noted that, in the case of electronic transfers, typically made via online banking, the place of commission is the same as the place where the person initiating the transaction carried out the act. If this place is located abroad and the predicate offense is also suspected to have been committed abroad, then the

²⁵ Supplemented by Prosecutorial Circulars TPK.1008/2017/37-I and TPK.1008/2017/37-II.

territorial and personal jurisdiction of the Criminal Code must be examined in particular in relation to the investigation conducted on suspicion of money laundering (Hungarian jurisdiction must be examined separately in relation to the predicate offense and the related money laundering).

In most cases, it is not expedient to investigate crimes committed abroad by foreign nationals in Hungary, but if circumstances nevertheless justify conducting an investigation in Hungary, the initiation of criminal proceedings shall be ordered by the Prosecutor General pursuant to Section 3(3) of the ACC.

The Public Prosecutor's Office also took the position that the interrogation of so-called financial agents as witnesses is unlawful and, from a criminal tactics point of view, a flawed practice, since the conduct of such persons and their criminal liability should be examined as perpetrators of money laundering. During questioning as a witness, a person against whom there are well-founded suspicions of criminal activity may become aware of the ongoing investigation.

3. ENFORCEMENT PRACTICE AND THE ROLE OF FINANCIAL AGENTS

3.1. Practical experiences

Practice shows that in some cases the predicate offense is committed abroad by a foreign perpetrator, thus necessitating international criminal cooperation. Evidence that can be used in criminal proceedings can only be obtained through judicial cooperation. In addition to direct legal assistance channels, Eurojust is a forum for judicial co-operation, which can be accessed by the investigating authority through the public prosecutor's office. In addition to direct requests, it is also advisable to request data from financial service providers through the NTCA FIU, which also has links with countries outside the EU. In addition, the International Law Enforcement Cooperation Center (hereinafter: ILECC), which functions as an organizational element of the Hungarian National Police Headquarters, also provides channels for police cooperation (Europol and Interpol Hungarian Liaison Office), through which it is possible to exchange information directly with partner offices.²⁶

²⁶ For further details, see: 25/2017. (VIII. 17.) ORFK utasítás az Európai Rendőrségi Hivatal által működtetett Európai Biztonságos Hálózat alkalmazásainak felhasználásával megvalósuló együttműködés és információcsere rendjéről szóló 23/2016. (IX. 15.) BM–NGM együttes utasítás végrehajtásáról [Instruction of the National Police Headquarters on the implementation of Joint Instruction No. 23/2016 (IX. 15.) of BM–NGM on the

In addition to the above, it is also possible to obtain data and information informally from foreign judicial/law enforcement partner agencies, however, even in these cases, it is not possible to dispense with the initiation of a request for legal assistance (it is another matter that in the case of countries with which there is no reciprocity, or which, based on experience, would not comply with the request for legal assistance, or would do so only after a significant delay, no other data may be available apart from that obtained informally).

Experience shows that in the case of the method of committing the offense referred to as a financial agent or money courier ("money mule"), the basic act is usually committed in a foreign country, in many cases far away, outside Europe, using data obtained through an attack launched by means of a computer device. Identifying the perpetrator of the predicate offense is extremely time-consuming and costly, and would require law enforcement authorities to perform an impossible and, in the absence of jurisdiction, unnecessary task. As long as there is no evidence that a person who could be considered a defendant in a Hungarian criminal case – typically someone who has access to the account to which the money obtained through fraud is transferred – participated in the commission of the predicate offense, intentional conduct that could be considered money laundering should be assessed within the framework of Sections 399(1) and (2) of the ACC. The court of first instance did not assess the evidence in this regard.

3.2. The importance of seizure

Criminal proceedings must also cover the investigation of assets acquired through criminal activity and the application of coercive measures and sanctions of a financial nature.²⁷ The order of priority for seizure is as follows: first, assets credited to accounts, then cash, and only then movable property. Real estate may be used as security if the measures taken to recover damages are insufficient or unsuccessful.

If Hungarian jurisdiction does not extend to the criminal proceedings for the predicate offense, this does not in itself prevent the seized money from being

procedure for cooperation and information exchange using the applications of the European Secure Network operated by the European Police Office], Hivatalos Értesítő 2017/40.

²⁷ This is stipulated in Section 353 of the ACP, as well as in 20/2018 (V. 31.) ORFK utasítás a bűncselekményekből származó jövedelmek és a bűncselekményekhez kapcsolódó egyéb javak felkutatása, azonosítása és a vagyonzbiztosítás érdekében teendő feladatokról (Instruction of the National Police Headquarters on the search for and identification of income derived from criminal offenses and other assets related to criminal offenses, and on tasks to be performed for the purpose of securing assets), Hivatalos Értesítő 2018/21.

released to the foreign victim, as the new crime committed against the object of the predicate offense against property (money laundering) does not affect the owner, and therefore does not affect the order of release following the termination of the seizure. In such cases, the object of the money laundering is the same as the object of the predicate offense, and there can be no confiscation of property, as this would make it impossible for the victim of the predicate offense to obtain compensation for the damage to their property rights.

3.3. Social engineering fraud

Nowadays, one of the typical methods of fraud is the so called social engineering fraud. Social engineering, or psychological manipulation, is when an authorized person transfers data to an unauthorized user or provides access to the system due to the deceptive behavior of the other person. Psychological manipulation is a type of attack in which the perpetrator does not exploit technological vulnerabilities, but rather uses human susceptibility as their main weapon. The most common form in international practice is Business Email Compromise (BEC/CEO fraud) as a prevalent form of international cyber-enabled fraud. Perpetrators typically hack into IT systems and trick employees responsible for financial transactions at the victim organization (business) into executing transfers according to false or forged payment instructions sent by them. Usually, they send a payment instruction on behalf of the partner from an email address created by the perpetrators that appears to be identical to the business partner's email address, requesting the fulfillment of a payment obligation relating to the actual business relationship to the company's changed payment account number, which is already under the control of the perpetrators. The crime can be committed not only with an email address similar to that of the financial partner, but also with their actual email address, by gaining unauthorized access to their account (compromising it). The methods used to commit these crimes are constantly changing, and nowadays there are also methods of fraud committed on a massive scale on social media and online marketplaces. Its significance, in connection with the commission of the basic act of money laundering, is outstanding.

4. INTERNATIONAL COOPERATION AND ASSET RECOVERY

In a significant proportion of cases, using the above mentioned social engineering fraud, as well as straw men, and in connection with drug trafficking or corruption, more serious, organized crime, the National Police Headquarters has prepared

another methodological guide under its professional supervision, which requires investigating authorities to carry out the following procedural actions:

- Pursuant to Section 368(1)(a) of the ACP,²⁸ the investigating authority is obliged, without a decision and regardless of its powers and jurisdiction, to carry out urgent investigative actions that cannot be postponed and may carry out any evidentiary acts that it would otherwise be authorized to order, and then send the resulting documents to the investigative authority with jurisdiction and competence.

In this context, if the target account is held by a financial institution operating in Hungary, immediate action must be taken to seize the incriminated amount for the purposes of indemnification. If it has already been withdrawn in cash, an immediate attempt must be made to seize it from the person concerned. In addition, if it is necessary to contact the domestic financial institution to obtain documents relating to the account or online banking data used, a request for information must be sent to it. The account-holding financial institution can be identified based on the first eight digits of the account number, for which several online platforms are available (e.g. bankkereso.eu). It is advisable to carry out the data request as an urgent investigative action [Section 262(3) of the ACP], as obtaining the prosecutor's permission would cause an unreasonable delay that would jeopardize the identification of the perpetrator or the collection of evidence. The following may be carried out within the framework of the data request: obtaining data related to the account number, identifying the characteristics of the accounting, payment and/or settlement system, suspending the operation, identifying suspicious financial partners, collecting data related to the beneficiary and listing the locations of cash withdrawals.

In case if the target account is held at a financial institution operating abroad, the investigating authority shall, also for the purpose of securing assets, send an urgent request to the NTCA FIU²⁹ in order to send a request to the foreign partner authority and to request the suspension of the transaction³⁰ from the foreign partner authority. The NTCA FIU shall

²⁸ Also based on Section 6(1) of 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről (Minister of Interior Decree on the powers and jurisdiction of police investigative authorities), Magyar Közlöny 2013/104.

²⁹ Pursuant to Section 48(4) of AML/CFT Act, authorities to which the NTCA FIU may independently forward information are entitled to send requests for the provision of information.

³⁰ The NTCA FIU can provide information on whether the national legislation of the requested country allows for the suspension of transactions, and on the time period during which it can maintain property insurance.

request the suspension of the transaction if, based on the facts of the case, the investigating authority's request establishes a suspicion of money laundering or an organized property-generating crime and the transfer to the foreign target account took place within three days.

If the investigating authority also requested the suspension of the transaction by the foreign partner authority in its request, this must be followed by the issuance of a European Investigation Order (hereinafter: EIO) or a request used in the Act on criminal cooperation with Member States of the European Union.³¹ It is important to note that neither reciprocity nor double criminality is a general condition for criminal cooperation with EU Member States. The Act however, applies the principle of double discrimination to some extent to certain forms of cooperation with other EU Member States.³²

According to the Act on International Legal Assistance in Criminal Matters³³ international treaties have priority compared to the application of the domestic regulation. Hungary has plentiful bi- and multilateral convention related to cooperation in criminal matters with other countries.³⁴ The confiscation of assets and freezing³⁵ for the purpose of compensating the victim for damage and/or financial loss does not fall within the scope of the EIO Directive and is only possible by means of a request for legal assistance or a decision ordering the freezing of assets.³⁶

- In order to obtain or change cross-border data and information, it is also necessary to involve ILECC, which may justify sending a request or submitting a request for legal assistance to the law enforcement authorities of the country concerned through European Police Office (hereinafter: Europol) and International Criminal Police Organization (hereinafter: Interpol) channels. Data obtained through informal channels can simplify and speed up requests for legal assistance, as data obtained through the SIENA system operated by the Europol, which ensures

³¹ 2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről (Act on criminal cooperation with Member States of the European Union), Magyar Közlöny 2012/160.

³² Ligeti, K., *A Nemzetközi Bűnügyi Együttműködés Általános Feltételei (General Conditions for International Criminal Cooperation)*, in *Az Európai Bűntetőjog Kézikönyve (Handbook of European Criminal Law)*, ed.: Kondorosi, F.; Ligeti, K., Magyar Közlöny Lap- és Könyvkiadó, Budapest 2008, pp. 59-85, 76.

³³ 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről szóló (Act on international legal assistance in criminal matters), Magyar Közlöny 1996/54. sz.

³⁴ Köhalmi, L., *A Nemzetközi Bűnügyi Együttműködés (International Criminal Cooperation)*, in *Magyar Bűntetőjog Általános Rész (Hungarian Criminal Law General Part)*, ed.: Tóth, M.; Balogh, Á., Osiris, Budapest 2010, pp. 375-386, 376.

³⁵ This legal institution has been in force since December 19.

³⁶ Practical advantages of involving the NTCA FIU in urgent asset-freezing cases.

secure information exchange, can be obtained through a request for legal assistance and thus used in open proceedings.

Within ILECC, the Europol Hungarian Liaison Office carries out and supervises the exchange of information and the sending of requests within the framework of the above-mentioned Instruction No. 25/2017 (VIII.17.) of the National Police Headquarters. Based on this, several units were granted full access, and end-point users are able to engage in cross-border cooperation with partner agencies directly, without the involvement of the liaison office.

Europol has a separate unit dedicated to cybercrime (European Cybercrime Centre-EC3). Its work is carried out through three main analytical projects such as AP Cyborg, AP Twins and AP Terminal. Representing Hungary, the National Bureau of Investigation of the Riot Police³⁷ is a member of all three projects.

Interpol, which currently has 192 member countries, can mainly assist in the fight against cybercrime through international criminal cooperation with third countries. Information can be exchanged with Interpol via the "Interpol channel", typically with non-EU countries. The Hungarian National Office of Interpol, operating within the organizational framework of ILECC is authorized to maintain contact.

Liaison offices³⁸ also enable the direct exchange of data and information, among which the cybercrime liaison points are particularly noteworthy, through which the countries participating in the network operate a continuous, so-called non-stop on-call system for receiving and sending requests. Basically, ILECC is the designated 24/7 contact point, while the National Bureau of Investigation of the Riot Police acts as the professional contact point.

Cross-border data exchange through the network of liaison officers³⁹ – Europol Hungarian Liaison Office (Netherlands), Germany, Serbia,

³⁷ The Riot Police operates under the direct control of the National Police Headquarters – specifically, the Chief of the National Police – with independent tasks and powers, national jurisdiction, and as an independent central budgetary agency, in accordance with the tasks and powers specified in Section 9 of 329/2007. (XII. 13.) Korm. rendelet a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről (Government Decree on the Police and the tasks and powers of the Police), Magyar Közlöny 2007/174.

³⁸ Details regarding the rapid international exchange of information provided by the Liaison Offices (competent offices, mandatory elements of requests, areas of cooperation and information exchange) are available on the internal intranet website of the National Police Headquarters. For more details, see 11/2024. (III. 21.) ORFK utasítás a kapcsolattartási szolgálati helyek működéséről (Instruction of the National Police Headquarters on the operation of liaison offices), Hivatalos Értesítő 2024/16.

³⁹ For more details, visit <https://www.police.hu/hu/a-rendorsegrol/testulet/teruleti-szervek/nemzetkozi-bunugyi-egyuttmukodesi-kozpont>, 8 January, 2026.

United Kingdom and Southeast European Law Enforcement Center (SELEC) – can also support the success of the proceedings.⁴⁰

- In cases where reports are filed on the basis of a simple suspicion of a criminal offense, an investigation must be ordered within the time limit prescribed by law; there can be no supplementation or rejection of the report. In cases of online fraud, to identify the perpetrator(s) during the investigation, it is essential to save the original source (addressee) of the misleading electronic message sent by the perpetrator(s) and then analyze the email header data. This helps to determine the sender's IP address, which must be checked to see if it is connected to the TOR⁴¹ network or to a VPS or VPN service⁴², the exact time the message was sent and received, the SMTP servers used by the sender and recipient and if the message has an attachment (e.g., a PDF file), what metadata it contains. If the message came from an IP address that can be linked to a subscriber, a request must be sent to the service provider managing the IP address to obtain the subscriber's data. In most cases, the service provider managing the IP address can be checked on public and free online platforms (e.g., whois.domaintools.com). Subsequently, data collection must be carried out in relation to the persons registered at the service address. If the IP address is used by multiple subscribers, all available data must be obtained, and then a narrowing search should be performed. This investigation must be carried out for all IP addresses that can be linked to the perpetrator or the act.
- In parallel with the analysis of technical data, it is advisable to interview persons who have been in contact with the perpetrator (e.g., who received an email or phone call) regarding circumstances that may help identify the perpetrator (e.g., in the case of a phone call: language, accent, gender, tone of voice, manner of expression). During the interview, other

⁴⁰Requests sent in parallel, mainly through international police cooperation channels, result in duplication in processing and, in the vast majority of cases, do not lead to the seizure of funds within a short period of time. In the countries requested, a court order is usually required to seize the money, and judicial authorization is also required to obtain bank data. The ILECC International Information Department has therefore drawn the attention of the investigating authorities to the fact that if the primary objective is to obtain evidence or ensure confiscation, EIO should be used.

⁴¹ The purpose of the TOR network is to encrypt user traffic and hide its source. Data traffic within the network is encrypted and takes place through a chain of interconnected computers, within which a given computer can only see the one computer in front of it and the one behind it, so the device behind the IP addresses recorded during the attack does not have information about the actual sender, meaning that it is not possible to identify the perpetrator based on the IP address.

⁴² In this case, you should contact your VPN or VPS provider to find out whether they store data related to your IP address.

technical data (e.g., phone number) and practices related to transfers/payments, as well as the financial transaction rights of each person, should be clarified.

- Based on the cash flow data obtained, data collection must be carried out on all persons (or business entities) who can be linked to the account or the transaction in question. This may include: the person who initiated the account opening (or who was present⁴³ with that person at the time in the bank branch), the co-cardholder, the legal representative, the senior officer, and the delivery agent.

With regard to the notification telephone number provided to the financial institution, a request for data must be made to the relevant mobile service provider to obtain subscriber data, call logs, cell information, SIM cards associated with the calling number, and subscriber data, call logs, and cell information associated with these SIM cards. Subsequently, the address provided must be verified and a search must be carried out as a coercive measure.

- It may also be justified to contact the Asset Recovery Office of the National Bureau of Investigation of the Riot Police (hereinafter: ARO) in order to verify any other data that may arise in the case and to map the assets derived from the crime. The asset recovery offices of the European Union, the Camden Asset Recovery Inter-Agency Network (CARIN) and the countries that have joined regional organizations modeled on it, through the ARO, can in many cases effectively support the tracking of amounts derived from fraud and the recovery of damages. In order to explore the possibilities, it is advisable to consult with the ARO in advance.
- Based on a text search in criminal case processing databases, background research must not be omitted during the investigation. A beneficiary's bank account number may also be involved in other domestic criminal proceedings, in which case substantive information may already be available regarding the account and the perpetrators, and further connections may also be uncovered. The search must be extended to the TakarNet Land Registry Information System, the domestic and international company information system, the personal and address register, the vehicle registry, the registry of member state judgments, the wanted persons registry, the criminal registry, and the weapons registry.
- If, following the imposition of coercive measures restricting property rights abroad, the property is not transferred within a short period of time, it is advisable to find out whether the domestic law enforcement

⁴³ The seizure of camera recordings made at the bank branch is definitely justified.

authorities expect to receive information at regular intervals regarding the need to maintain the coercive measures.

- If the perpetrator has opened a bank account using a false ID card in the name of another existing person or a photo ID card created with the details of a non-existent person, to establish their identity, the photo on the ID card used to open the account or, if available, a photo of sufficient quality taken at the time of opening the account at the bank branch (or during a cash withdrawal from an ATM), these must be uploaded to the facial recognition system. If the facial recognition system returns a match for a person from a country neighboring Hungary, a request must be sent to the competent Liaison Office to verify the data of the person concerned and obtain their photograph. In certain cases, establishing the identity of the perpetrator may also justify sending a request to the Deputy State Secretariat for Registers of the Ministry of the Interior in order to compile a family tree of the suspects.
- With regard to the perpetrators (straw men), a request must be sent to all Hungarian credit institutions to determine whether they have Hungarian bank accounts, and requests must also be sent to Hungarian telecommunications service providers to determine whether they have Hungarian telephone numbers. In addition to the above, the persons concerned must be checked on social networking sites in order to map their circle of relatives and friends. In the case of an identified perpetrator who is reasonably suspected of having committed the crime, it is essential to obtain information about their criminal record. Based on this, the identity of perpetrators and accomplices previously unknown to the investigating authorities may also be revealed.
- Foreign business organizations potentially involved in money laundering must also be checked in foreign company registers. It may also be necessary to send a request via the ILECC channel to foreign partner authorities to check the bank account numbers, natural and legal persons, telephone numbers, IP and e-mail addresses involved in the case. It is also essential to check whether the suspect used money transfer services outside the banking sector (e.g., Western Union, MoneyGram, etc.). If so, these service providers must also be contacted.
- In order to effectively detect crimes, apprehend perpetrators, secure material evidence, and conduct proceedings successfully and in a timely manner, it may be necessary to set up a joint investigation team (JIT) with the relevant foreign law enforcement authorities. To this end, a proposal must be made to the public prosecutor's office supervising the investigation.

5. CONCLUSION

The effectiveness of anti-money laundering measures is currently one of the most important issues in terms of upholding the rule of law, economic stability, and public trust.

In summary, as a result of the significant measures outlined in the action plan adopted following the Moneyval country report, police and prosecutorial practices regarding criminal proceedings initiated on suspicion of money laundering have been established and standardized in Hungary (at least during the investigative phase), and the necessary organizational and human infrastructure has been put in place. As a result of all this, the conduct of criminal proceedings and the implementation of measures to recover damages caused by the crime have become a kind of routine, which also had a positive impact on the duration of proceedings. The amendment to substantive criminal law broadened the scope of criminal activities, thereby making it easier for the authorities to assess such activities. Furthermore, by using the concept of "property" instead of the previous concept of "thing", the criminal law now includes objects of criminal conduct such as electronic money or cryptocurrency within the scope of seizure. Linking money laundering to the value of the criminal offense has also clarified the jurisdictional issues for the authorities involved, furthermore, all preparatory acts have become punishable, not merely the agreement to commit money laundering.

Given the international nature of money laundering, cross-border exchange of criminal intelligence and cooperation are indispensable; without them, effective detection and asset recovery are out of the question.

The primary scene for judicial and law enforcement cooperation consists of various channels, including Europol, Eurojust, Interpol, liaison offices, and joint investigation teams established with the participation of foreign judicial authorities.

The legal and institutional framework for combating money laundering in Hungary now rests on a solid foundation and is suitable for managing money laundering risks. In the future, however, the focus should not primarily be on creating new rules, but rather on making more effective use of existing tools, strengthening and enhancing cooperation between institutions, and improving the practical effectiveness of law enforcement. Only together can these measures ensure that the fight against money laundering not only formally meets international and domestic expectations but also effectively strengthens the rule of law and the integrity of the economy.

The measures outlined above have clearly yielded results: investigative authorities are successfully uncovering an increasing number of crimes, alongside a growing volume of restitution for damages during their proceedings, which gives cause for optimism when planning future actions against this phenomenon.⁴⁴

REFERENCES

BOOKS AND ARTICLES

1. Belovics, E.; Molnár, G.; Sinku, P., *Büntetőjog II., Különös Rész (Criminal Law II., Special Part)*, ed.: Belovics, E., HVG-ORAC, Budapest 2021, p. 827.
2. Földvári, J.; Gál, I. L., *Magyar büntetőjog, Általános Rész (Hungarian Criminal Law, General Part)*, Osiris, Budapest 2024, p. 316.
3. Gál, I. L., ed., *Magyar büntetőjog, Különös Rész (Hungarian Criminal Law, Special Part)*, Osiris, Budapest 2023, p. 511.
4. Gál, I. L., *Dogmatikai problémák a pénzmosás hatályos magyar szabályozásával kapcsolatban (Dogmatic problems related to the current Hungarian regulations on money laundering)*, *Belügyi Szemle*, 71. évfolyam, 2023/5., pp. 741–763.
5. Kóhalmi, L., *A Nemzetközi Bűnügyi Együttműködés (International Criminal Cooperation)*, in *Magyar Büntetőjog Általános Rész (Hungarian Criminal Law General Part)*, ed.: Tóth, M.; Balogh, Á., Osiris, Budapest 2010, pp. 375-386, 376.
6. Ligeti, K., *A Nemzetközi Bűnügyi Együttműködés Általános Feltételei (General Conditions for International Criminal Cooperation)*, in *Az Európai Büntetőjog Kézikönyve (Handbook of European Criminal Law)*, ed.: Kondorosi, F.; Ligeti, K., Magyar Közlöny Lap- és Könyvkiadó, Budapest 2008, pp. 59-85, 76.
7. Pintér, B., *A pénzmosás elleni küzdelem az új magyar büntető törvénykönyvben (Combating Money Laundering in the New Hungarian Criminal Law)*, doktori értekezés (doctoral thesis), Pécsi Tudományegyetem, Pécs 2012, p. 2.

⁴⁴ According to data from the Unified Investigative Authority and Prosecutor's Office Crime Statistics, the investigation success rate ranged between 87.8% and 92.3% between 2020 and 2024, which can be considered extremely good.

LEGAL ACTS

1. Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284 of 12/11/2018.
2. 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről (Act on international legal assistance in criminal matters), Magyar Közlöny 1996/54.
3. 2009. évi LXXXV. törvény a pénzforgalmi szolgáltatás nyújtásáról (Act on the provision of payment services), Magyar Közlöny 2009/100.
4. 2012. évi C. törvény a Büntető Törvénykönyvről (Act on the Criminal Code), Magyar Közlöny 2012/92.
5. 2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről (Act on criminal cooperation with Member States of the European Union), Magyar Közlöny 2012/160.
6. 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (Act on Credit Institutions and Financial Enterprises), Magyar Közlöny 2013/217.
7. 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról (Act on the prevention and combating of money laundering and terrorist financing), Magyar Közlöny 2017/75.
8. 2017. évi XC. törvény a büntetőeljárásról (Act on Criminal Procedure), Magyar Közlöny 2017/99.
9. 2020. évi XLIII. törvény a büntetőeljárásról szóló törvény és más kapcsolódó törvények módosításáról (Act on amending the Criminal Procedure Act and other related acts), Magyar Közlöny 2020/129.
10. 329/2007. (XII. 13.) Korm. rendelet a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről (Government Decree on the Police and the tasks and powers of the Police), Magyar Közlöny 2007/174.
11. 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről (Minister of the Interior Decree on the powers and jurisdiction of police investigative authorities), Magyar Közlöny 2013/104.
12. 1688/2017. (IX. 22.) Korm. határozat az Európa Tanács Moneyval országjelentésben Magyarország részére megfogalmazott pénzmosás elleni ajánlások végrehajtásáról készített akciótervről (Government Resolution on the action plan for implementing the recommendations against money laundering made to Hungary by the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism), Magyar Közlöny 2017/153.
13. 1691/2018. (XII. 17.) Korm. határozat a pénzmosás és terrorizmus finanszírozása elleni nemzeti kockázátértékelés felülvizsgálata

eredményképp megfogalmazott intézkedésekről (Government Resolution on measures formulated as a result of the review of the national risk assessment for money laundering and terrorist financing), Magyar Közlöny 2018/201.

14. 25/2017. (VIII. 17.) ORFK utasítás az Európai Rendőrségi Hivatal által működtetett Európai Biztonságos Hálózat alkalmazásainak felhasználásával megvalósuló együttműködés és információcsere rendjéről szóló 23/2016. (IX. 15.) BM-NGM együttes utasítás végrehajtásáról (Instruction of the National Police Headquarters on the implementation of Joint Instruction 23/2016 (IX. 15.) BM-NGM on the procedure for cooperation and information exchange using the applications of the European Secure Network operated by the European Police Office), Hivatalos Értesítő 2017/40.
15. 20/2018 (V. 31.) ORFK utasítás a bűncselekményekből származó jövedelmek és a bűncselekményekhez kapcsolódó egyéb javak felkutatása, azonosítása és a vagyónbiztosítás érdekében teendő feladatokról (Instruction of the National Police Headquarters on the search for and identification of income derived from criminal offenses and other assets related to criminal offenses, and on tasks to be performed for the purpose of securing assets), Hivatalos Értesítő 2018/21.
16. 11/2024. (III. 21.) ORFK utasítás a kapcsolattartási szolgálati helyek működéséről (Instruction of the National Police Headquarters on the operation of liaison offices), Hivatalos Értesítő 2024/16.
17. Circular of Department of Priority and Military Cases of the Hungarian Prosecutor General's Office No. KF.9725/2004/379-II, No. TPK.1008/2017/37-I. and No. TPK.1008/2017/37-II.
18. Information note for the purpose of informing members of parliament, Office of the National Assembly, Public Collections and Public Education Directorate, Representative Information Service 2025/18 (May 30, 2025).

COURT PRACTICE

1. Hungarian Supreme Court decision No. BH 2019.125.

NETWORK RESOURCES

1. <https://www.police.hu/hu/a-rendorsegrol/testulet/teruleti-szervek/nemzetkozi-bunugyi-egyuttmukodesi-kozpont>, 8 January, 2026.

2. <https://www.mnb.hu/felugyelet/szabalyozas/penzmosas-ellen/korlatozo-intezkedesek-szankciok/penzugyi-akciocsoport-fatf>, 14 January, 2026.

UDK: 343.6 : 614.253

(497.5)

Review paper

Hrvoje Bralić, PhD student

Faculty of Law, University of Split, Croatia

E-mail: bralic.hrvoje@gmail.com

ORCID: 0009-0000-6006-3650

CAUSATION IN THE CRIMINAL OFFENSE OF NEGLIGENT MEDICAL TREATMENT IN LEGAL DOCTRINE AND CROATIAN CASE LAW

ABSTRACT

The concept of causation in criminal law is a complex and difficult-to-define legal institute. Three theories prevail: the theory of equivalence, the theory of adequacy, and the theory of objective imputation. The criminal offense of negligent medical treatment constitutes a wrongful act by omission. A causal link exists only if the required action would have prevented the consequence. Complexity arises when, despite negligent treatment and the created risk, the same consequence occurs, raising the issue of applying the doctrine of permissible alternative conduct. Advances in medicine and technology have increased treatment risks, while the law seeks stronger protection of the right to health. Although outcomes of certain medical interventions are often known, negative consequences may occur even with proper conduct and adherence to professional standards. Scientific uncertainty must be accommodated within criminal law norms, which require a high degree of legal certainty. Croatian case law shows that courts, following the theory of objective imputation, demand a high—and often higher—degree of certainty than that proposed by legal theory. This approach aligns with the purpose of the offense of negligent medical treatment and contemporary medical developments, as it limits criminal liability to serious and obvious cases of malpractice that, with near-complete certainty, result in the deterioration of the patient's health, while preventing the further emergence of defensive medicine. This paper defines the criminal offense of negligent medical treatment, reviews the notion of causation, and analyzes Croatian legal theory and case law, drawing conclusions about their consistency and examining whether the ratio legis of the offense has been achieved.

Keywords: criminal law, causation, negligent medical treatment, defensive medicine

1. INTRODUCTION

The concept of causation generally represents a challenge that gives rise to numerous questions and debates. Due to its specificity in each individual and concrete situation, the notion of causation is almost impossible to define unequivocally. It is the subject of discussion in both the natural and the social sciences and poses difficulties in the natural sciences as well as in the humanities. Its complexity in attempts at definition has resulted in the fact that, within contemporary Croatian criminal law, there is no normative definition of causation, even though it constitutes an objective element of a criminal offence.

Although no normative definition exists, this paper analyses the concept of causation in the criminal offence of negligent medical treatment in legal theory and Croatian judicial practice, with the aim of examining the circumstances in which a medical professional who acts contrary to the rules of the profession incurs criminal liability. The existence of a clear distinction in this respect ensures effective protection of the right to health, while at the same time enabling medical professionals to perform their specific professional duties under conditions of legal certainty. Excessive criminalisation would otherwise render the medical profession impossible to practise in a legally secure manner. Physicians' fear of litigation has led to the development of a practice known as defensive medicine, defined as the ordering of unnecessary diagnostic tests and procedures or the avoidance of treating patients considered high-risk.¹ For these reasons, the existence of a clear normative and judicial framework is essential in order to achieve a balance between two competing objectives: the protection of human health and the unimpeded exercise of the medical profession. Accordingly, following the entry into force of the new Criminal Code on 1 January 2013, the legal definition of the offence of negligent medical treatment was structured so as to sanction only manifest breaches of professional standards, evidently negligent conduct, or the failure to implement measures for the protection of patients, with the aim of ensuring that this offence operates strictly as an *ultima ratio*.² This paper examines recent judicial practice concerning the issue of causation in relation to the aforementioned offence, analysing it through the lens of theoretical legal models, with a view to determining whether case law has kept pace with legislative

¹ Miziara I.D., Miziara C.S.M.G., *Medical errors, medical negligence and defensive medicine: A narrative review*, Clinics, Universidade de Sao Paulo, Brazil, 2022., p. 1

² Roksandić Vidlička S., Pražetina Kaleb R., *Utvrdjivanje pravnog kontinuiteta i tumačenje elemenata bića kaznenog djela nesavjesnog liječenja*, Zbornik radova s međunarodnog kongresa: "1. kongres KoKoZ-a i 3. hrvatski kongres medicinskog prava s međunarodnim sudjelovanjem, Pravni fakultet Sveučilišta u Splitu, 2019., p. 311.

developments in this area and whether the intended function of this offence as an *ultima ratio* has indeed been realised.

The paper defines the criminal offence of negligent medical treatment, provides an overview of the concept of causation, and ultimately analyses Croatian legal theory and judicial practice. It offers conclusions regarding their consistency and examines the application of the criminal offence of negligent medical treatment in case law, addressing the question of whether the ratio legis of the offence has been fulfilled and assessing its effects in relation to the concept of defensive medicine.

2. THE CRIMINAL OFFENCE OF NEGLIGENT MEDICAL TREATMENT

The criminal offence of negligent medical treatment is statutorily defined in Article 181 of the Criminal Code.³ This offence constitutes a *delictum proprium*. As is evident from paragraph 1, the circle of potential perpetrators includes healthcare professionals. The term healthcare professionals refers to physicians, doctors of dental medicine, medical biochemists, nurses and medical technicians, pharmacists, physiotherapists, sanitary engineers, and other professions listed in the Act on Healthcare Professions.⁴

Persons possessing the aforementioned status must, in the performance of healthcare activities, apply an obviously inappropriate means or method of treatment, or otherwise manifestly fail to act in accordance with the rules of the medical profession, or act in an obviously negligent manner.

When classifying the criminal offence of negligent medical treatment with regard to the structure of the offence, it is evident that this is an offence of injury. The injury consists in the violation of the protected legal good, namely human health. The violation is concretised, in the basic form of the offence, by the worsening of an illness or the impairment of another person's health. In the qualified forms of the offence, it is required that the conduct result in particularly serious bodily injury, termination of pregnancy, or the death of one or more persons.

³ Criminal Code of the Republic of Croatia ("Official Gazette" br. 125/11., 144/12., 56/15., 61/15., 101/17., 118/18., 126/19., 84/21., 114/22., 114/23., 36/24, 136/25)

⁴ Cvitanović L., et al., *Kazneno pravo posebni dio*, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2018.

The injury thus concretised represents the consequence, the cause of which is the manifestly negligent conduct or omission of the healthcare professional. The consequence is a highly significant element of this criminal offense, as the type and severity of the consequence directly determine the gravity of the offense itself, as well as the range of penalties available to the court if the defendant is found guilty.⁵ It follows that this is a material criminal offence. From the statutory description, it is clear that the criminal offence of negligent medical treatment may be committed by commission (the application of an obviously inappropriate means or method of treatment) and by omission (manifest failure to act in accordance with the rules of the profession or otherwise manifestly negligent conduct). Where an offence may be committed both by commission and omission, it is defined as an improper omission offence;⁶ accordingly, the criminal offence of negligent medical treatment is classified also as an improper omission offence.

The criminal offence of negligent medical treatment medical treatment may be committed with intent or through negligence. Intent is possible only with regard to the negligent manner of treatment. It exists where the perpetrator is aware that he or she is acting contrary to the rules of the profession and wishes to act in such a manner (direct intent of the first degree); where the perpetrator is certain that a particular course of conduct will violate professional rules and nevertheless undertakes it (direct intent of the second degree); or where the perpetrator is not entirely certain that the conduct is contrary to professional rules but accepts such a possibility and proceeds regardless (indirect intent).⁷

Advances in medical science and technological development have simultaneously increased the risks inherent in medical treatment, thereby automatically increasing the responsibility of healthcare professionals who provide treatment and healthcare protection.⁸ On the other hand, the development of law has resulted in the enactment of numerous legal provisions guaranteeing individuals the right to healthcare and, in connection therewith, the right to the protection of life and bodily integrity in the course of receiving such care. The objective is to reconcile these two developmental trends. If the standard of liability is set excessively high, one may speak of a tendency toward the establishment of objective liability, which is inconsistent with the development and achievements of criminal law. For this

⁵ Mrčela M., Vuletić I., *Liječnik i kazneno pravo*, Narodne novine, 2019., p. 17.

⁶ Martinović I., *O kriteriju razlikovanja pravih i nepravih kaznenih djela nečinjenja*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 65 No. 1, 2015., p. 131.

⁷ Mrčela M., Vuletić I., *Granice nehajne odgovornosti za kazneno djelo nesavjesnog liječenja*, Zbornik radova Pravnog fakulteta u Splitu, 3, 2017., p. 689.

⁸ Roksandić Vidlička S., *Aktualna pitanja pojedinih kaznenih djela protiv zdravlja ljudi*, Hrestomatija hrvatskog medicinskog prava, Pravni fakultet sveučilišta u Zagrebu, 2016., p. 819.

reason, the element of reasonableness must remain an essential component in determining the applicable standard.⁹

Today, there is, on the one hand, a tendency to expand as far as possible the liability of healthcare professionals for harm; on the other hand, there are demands that, due to the specific characteristics of this professional activity, they be granted immunity from liability.¹⁰ For this reason, the Croatian Criminal Code confines entry into the criminal sphere exclusively to manifestly negligent acts and omissions. Contemporary tendencies prescribed at the legislative level are reflected in their practical application before Croatian courts. Thus, in 2018 there were 78 criminal complaints filed for the criminal offence of negligent medical treatment, of which 68 were dismissed, and no convictions were rendered. Accordingly, while the number of criminal complaints is increasing, the number of indictments remains small and the number of convictions even smaller.¹¹ One of the principal reasons for acquittals lies precisely in the question of the existence or absence of causation as an objective element of the criminal offence of negligent medical treatment.

3. CAUSATION

In material offences, causation constitutes an objective element of the criminal offence and consists in the fact that it was precisely the unlawful act that brought about the consequence prescribed by statute. The purpose of causation is to ensure that the perpetrator is held responsible for those changes in the external world that are the result of his or her conduct, but not for those that merely coincidentally follow upon it.¹² In philosophical literature, causal responsibility is attributed to an individual for an outcome when that individual's conduct causes the outcome.¹³ Throughout history, with the development of all sciences—particularly the natural sciences—the concept of causation has become increasingly complex. This is most clearly visible in the development of the natural sciences, especially physics, chemistry, biology, astronomy, and medicine. The culmination of this complexity

⁹ *Ibid.*, p. 829.

¹⁰ Mišić Radanović N., Vukušić I. *Odnos različitih vrsta deliktne odgovornosti zdravstvenih radnika*, Zbornik radova s međunarodnog kongresa "2. Kongres KOKOZA i 4. Hrvatski kongres medicinskog prava s međunarodnim sudjelovanjem", 2020.

¹¹ Mišić Radanović N., *Prijepori o kazenoj odgovornosti medicinskih djelatnika za stručnu pogrešku*, Godišnjak Akademije pravnih znanosti Hrvatske, Vol. XI. No. 1, 2020., p. 42.

¹² Novoselec P., Bojanić I., *Opći dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2013., pp. 150–151.

¹³ Firkins G., *Rethinking Causation in English Criminal Law*, The Journal of Criminal Law 2023, Vol. 87(1), 2023., p. 24.

is reflected in the theory of deterministic chaos. Deterministic chaos is defined as the unpredictable, chaotic behaviour of nonlinear dynamic systems governed by deterministic laws. At first glance, this appears paradoxical, as the concept intertwines two notions usually regarded as incompatible: determinism and chaos. Many systems behave in an unpredictable (chaotic) manner even though they are relatively simple, the forces acting upon them are known, and they are described by deterministic equations of motion.¹⁴ Although it may be possible to control the initial conditions of an event, over time the connection between those initial conditions and subsequent states of affairs weakens. Ultimately, over a sufficiently long period, the nonlinearity of the dynamic systems involved means that it is no longer possible to predict or model how an event will unfold. Consequently, the contribution of the initiator of an action becomes immeasurably small, leading to the conclusion that continuity is absent.¹⁵

For these reasons, causation in both the natural sciences and philosophy is increasingly viewed as a functional concept. Metaphysical interpretations are being abandoned, as is the classical deterministic, or deductive-nomological, model according to which causation is a real, empirical phenomenon that could, following Galileo's original conception, be fully expressed mathematically. Of course, the law cannot and need not concern itself with such physical subtleties. At the same time, it should not be misled into believing that causation in law can be ontologically grounded in various simplified formulae.¹⁶ Precisely because of the complexity of the concept of causation, there have been historical attempts to define it strictly or to absolutise it.

Two principal currents emerged in this regard. One is represented by traditional metaphysicians who, broadly speaking, continue the Cartesian tradition and classical German idealism. Their understanding of causality may be illustrated by Descartes' well-known statement that "nothing comes from nothing"; for them, the hierarchy of causes ultimately culminates in a final cause. The second current inclined toward the absolutisation of causation consists of proponents of the classical philosophical, Laplacean deterministic model of causation. For them, causation is measurable, indisputable, reducible to natural laws, and ultimately expressible in the formula *conditio sine qua non*.¹⁷

¹⁴ Croatian Encyclopedia, online edition, Miroslav Krleža Institute of Lexicography, 2013–2024, <https://www.enciklopedija.hr/>, 10 February 2026.

¹⁵ Simester, A., *Causation in (Criminal) Law*, Law Quarterly Review, 133(3), 2017., p. 420.

¹⁶ Martinović I., *Problem uzročnosti u kaznenom pravu*, Hrvatski ljetopis za kazneno pravo i praksu, Vol. 19 No. 1, 2012., p. 78.

¹⁷ *Ibid.* p. 86.

Just as other sciences have failed to provide a single, unequivocal concept of causation, criminal law theory has likewise not arrived at a uniform definition. Consequently, the Criminal Code contains no normative definition of causation. Three dominant theories have developed within criminal law doctrine.

The first is the theory of equivalence. Its criterion is purely natural-scientific (naturalistic): in determining causation, no selection of causes is made according to their legal significance, nor are they otherwise evaluated. No distinction is drawn between essential and non-essential, direct and indirect, or proximate and remote causes. It is commonly associated with the formula *conditio sine qua non*.¹⁸ The usual objection raised against this theory in criminal law doctrine is *regressus ad infinitum*, that is, the fact that the search for causes may extend infinitely into the past. It is therefore evident that the formula *conditio sine qua non* leads to absurd results; ultimately, it renders causally relevant virtually every human action in the entire history of humankind.¹⁹

In an attempt to overcome the shortcomings of the theory of equivalence, the theory of adequacy was developed. The theory of adequacy requires that the change in the external world must be a typical consequence of a given act. Human conduct must be, according to general experience, suitable to bring about a particular consequence—otherwise, causation does not exist. Roxin objects to this theory on the ground that it is not a genuine theory of causation, since it does not demonstrate when a circumstance is causal for a consequence, but rather attempts to answer the question of which causal circumstances are legally relevant and may be imputed to the perpetrator.²⁰

These two theories demonstrate that, due to their limitations—and given that they directly pertain to the constituent elements of a criminal offence—they result in indeterminacy, which is contrary to the principle of *lex certa*. Determinacy and foreseeability are necessary in order for citizens to understand and plan their conduct.²¹ In this context, the principle of the rule of law is likewise significant, as criminal liability may become excessively unpredictable if anyone who contributes to a prohibited outcome is exposed to criminal conviction.²²

¹⁸ Novoselec P., Bojanić I., *op. cit.*, note 12, p. 151.

¹⁹ Martinović I., *op. cit.*, note 16, p. 8

²⁰ *Ibid.*, pp. 84–85.

²¹ Vukušić I., *Lex certa u poredbenom pravu*, Zbornik radova pravnog fakulteta u Zagrebu, Vol. 73 No. 1., 2023.

²² Firkins G., *op. cit.*, note 13, p. 26

As a consequence of attempts to narrow causation as much as possible in a natural-scientific sense, while at the same time excluding the understanding of causation as purely legal causality, the theory of objective imputation emerged. This theory answers the question under what conditions a consequence will be objectively imputed to the perpetrator as his or her own act. If such imputation is not possible, the constituent elements of the criminal offence are not fulfilled.²³

According to this theory, conduct may be objectively imputed to the perpetrator where, by that conduct, a danger was created for the protected object which exceeded the limits of permissible risk, provided that precisely that danger materialised in the consequence prescribed by law as an element of the criminal offence.²⁴

4. CAUSATION AS A CONSTITUENT ELEMENT OF THE OFFENCE OF NEGLIGENT MEDICAL TREATMENT IN LEGAL THEORY

The criminal offence of negligent medical treatment, as previously noted, constitutes an offence of endangerment and a material criminal offence. Errors in diagnosis and therapy are necessary preconditions for criminal liability. However, even if such errors are established, this is still insufficient for a conviction. The prosecution must prove two additional requirements of liability: the occurrence of a consequence and the existence of a causal link between the medical errors and that consequence. The consequence may consist of an aggravation of the illness, a deterioration of health, termination of pregnancy, or the death of the patient.²⁵ Croatian legal theory adheres to the teaching of three fundamental theories of causation: the theory of equivalence, the theory of adequacy, and the theory of objective imputation.

In medicine, it is generally impossible to establish with absolute certainty that a particular medical error directly caused the consequence. In other words, a causal link between a medical error and injury to health or body, or the death of a patient, exists only if the court, on the basis of expert medical testimony, concludes that

²³ Novoselec P., Bojanić I., *op. cit.*, note 12, p. 15

²⁴ Martinović I., *op. cit.*, note 16, p. 93.

²⁵ Vuletić I., *Medical Malpractice as a Separate Criminal Offense: a Higher Degree of Patient Protection or Merely a Sword Above the Doctors' Heads? The Example of the Croatian Legislative Model and the Experiences of its Implementation*, *Medicine, Law & Society*, Vol. 12, No. 2, pp. 39–60, October 2019, p. 44.

treatment *lege artis* would have saved or prolonged the patient's life with a probability consistent with certainty. Probability consistent with certainty denotes a degree of certainty that excludes reasonable doubt.²⁶

Although the case law of European states generally accepts the theory of equivalence, the question nevertheless arises whether a criminal court may convict a physician if the harm suffered by the patient is characterised merely as a "loss of a chance of recovery or survival."²⁷ Due to the weaknesses of the theory of equivalence, and taking into account the specific nature of the constituent elements of the offence of negligent medical treatment, Croatian legal theory applies the theory of objective imputation to this particular offence.

According to this theory, conduct may be objectively imputed to the perpetrator where, by that conduct, a danger was created for the protected object that exceeded the limits of permissible risk, but only provided that precisely that danger materialised in the consequence prescribed by law as an element of the criminal offence. The first requirement is that the perpetrator exceeded the limits of permissible risk, thereby creating a danger to the protected object. The second requirement is the realisation of that risk in the consequence prescribed by law as an element of the criminal offence.²⁸ The consequence must reflect precisely the danger that arose due to the breach of the required standard of care.

This requirement will not be fulfilled if, had the perpetrator complied with the required standard of care (or in the case of so-called lawful alternative conduct), the same consequence would certainly have occurred. It should further be noted, bearing in mind the nature of the offence of negligent medical treatment, that in cases of improper offences by omission only hypothetical causality is possible. That is, omission and consequence may be regarded as lawfully connected only where the required action would have prevented the consequence. In this context, the formula *conditio sine qua non* is likewise applied, albeit in a modified form—not as a hypothetical process of eliminating an actually performed act, but as a hypothetical process of adding the omitted act. If it is established that the consequence would not have occurred, it is to be imputed to the perpetrator; if it would have occurred in any event, it is not to be imputed.²⁹

²⁶ Mišić Radanović N., Vukušić I., *Causation in medical malpractice, EU and Comparative Law Issues and Challenges Series* (ECLIC), 2020. p. 784.

²⁷ *Ibid.* p. 783.

²⁸ Martinović I., *op. cit.*, note 16, pp. 93–94.

²⁹ Novoselec P., Bojanić I., *op. cit.*, note 12, pp. 158–159.

The most controversial situation in which the risk does not materialise in the consequence prescribed by law is that in which the same consequence would have occurred even if the perpetrator had complied with the required standard of care (so-called lawful alternative conduct). Theoretically, however, it remains disputed what should be done where the court cannot determine with certainty what would have occurred had the perpetrator fulfilled the requirements of due care.

Roxin's theory of risk increase, as well as its variations, maintains that compliance with the prescribed standard of conduct should be insisted upon even where it does not protect the legal good with certainty, but merely increases the possibility of protection. Accordingly, Roxin argues that the consequence should be imputed to the perpetrator as soon as, by breaching the rules of proper conduct, he or she increases the legally relevant risk, that is, the danger of the occurrence of the consequence. Ambrož justifiably objects that, under this assumption, it becomes impossible to compare the perpetrator's conduct with the hypothetical lawful conduct. Nor should one accept Roxin's more extreme position, according to which the limitations of the court's epistemic capacities would effectively operate to the detriment of the accused.

From a criminal policy perspective, in such complex cases imputation should be limited to situations in which the risk has been increased in a legally relevant manner. What constitutes the precise threshold of such relevance remains an open question in legal theory.³⁰

5. CAUSATION AS A CONSTITUENT ELEMENT OF THE OFFENCE OF NEGLIGENT MEDICAL TREATMENT IN CROATIAN JUDICIAL PRACTICE

This paper analyses two criminal cases in which the issue of causation in the offence of negligent medical treatment was specifically addressed. The author conducted a search of all publicly available judicial decisions relating to the offence of negligent medical treatment in the case law database of the Supreme Court of the Republic of Croatia and additionally requested the delivery of final judgments in the same matters from the County Court in Zagreb and the County Court in Split. Through a review of the available decisions, the author established that the issue of causation in the offence of negligent medical treatment was problematised in only two judgments. The first case dates from 2012 and the second from 2022. By analysing these judgments, the paper seeks to determine

³⁰ Martinović I., *op. cit.*, note 16, p. 96.

which theory of causation Croatian courts apply in practice in cases concerning the criminal offence of negligent medical treatment.

In the first case, concluded by the judgment of the County Court in Bjelovar (No. KŽ-443/2011-3 of 16 February 2012), the accused, acting as the senior on-call surgeon, was charged with having failed to perform a complete clinical examination of a patient brought in after a traffic accident; despite radiological findings indicating a suspicion of aortic rupture, he failed to consult a cardiac surgeon in accordance with professional standards and did not arrange for the patient's urgent transfer to a specialised clinic in Zagreb. Nor did he undertake appropriate monitoring measures, even after the patient's condition deteriorated. As a result, the patient bled out due to a ruptured aorta and died.

In that case, the courts held that even if it were established that the accused had acted negligently, the results of the evidence did not support a reliable conclusion that the deterioration of the victim's health and his death were consequences of those omissions. From the complex expert opinion of the Faculty of Medicine of the University of Zagreb, it followed that mortality in operated cases of aortic rupture was up to 40%. Although a supplementary expert opinion indicated that mortality in cases involving injuries such as that sustained by the victim might be lower (15–20%), the court accepted the interpretation more favourable to the accused. It concluded that a 60% chance of survival did not provide a sufficient basis for establishing a causal link between the accused's omission and the fatal consequence, since it could not be reliably excluded that the same outcome would have occurred even if the victim had undergone surgery at the most favourable moment.³¹ The accused was therefore acquitted of the offence of negligent medical treatment.

This case demonstrates that Croatian judicial practice applies the theory of objective imputation. In cases of omission—such as the present one, which constitutes an improper offence by omission—only hypothetical causality is possible. It can never be asserted with absolute certainty that the omitted act would have prevented the consequence; probability therefore suffices. However, not just any degree of probability is sufficient. A high degree of probability, or probability bordering on certainty, is required. In the absence of such probability, the principle *in dubio pro reo* must be applied, and it must be assumed that the required act would not have prevented the consequence,³² that is, that causation is lacking.³³

³¹ Judgment of the County Court in Bjelovar, Case No. KŽ-443/2011-3, 26 February 2012.

³² Novoselec P., Bojanić I., *op. cit.*, note 12, pp. 159–160.

³³ Mrčela M., Vuletić I. *op. cit.*, note 5, p. 19.

In the second case, concluded by the judgment of the County Court in Zagreb (No. KŽ-634/2021-7 of 29 November 2022), the accused, an emergency physician, was charged with having examined an intoxicated person found lying on the road, determined that there were no visible injuries, and arranged for the person to be transported home rather than to hospital, despite the fact that the individual lived alone in neglected conditions. The following day, complications of a severe cranio-cerebral injury developed, resulting in death.

The appellate court held that the first-instance court had correctly acquitted the accused because it had properly found that the commission of the offence had not been proven with complete certainty. The evidence showed that, at the scene, the accused had detected no signs or symptoms indicating severe head trauma. The fact that such injuries were diagnosed the following day did not exclude the possibility that they had been sustained either before or after the examination. The crucial issue was the establishment of a causal link between the accused's conduct and the fatal consequence.

After analysing the entire proceedings, the appellate court agreed that it had not been proven with complete certainty that the accused's conduct, or the omissions attributed to him, were the acts that led to the harmful consequence. Nor was it established that the accused had failed to apply protective measures in accordance with the rules of the medical profession and that this omission subsequently resulted in the victim's death. The court further emphasised that it could not be disregarded whether the fatal outcome would have been avoided—and with what degree of certainty—had the victim been hospitalised, monitored, and operated on earlier, given the severity of the injury and other relevant factors such as age, general health, pre-existing conditions, and intoxication.³⁴

The first-instance court elaborated extensively on causation. It noted that the accused could not have known of the victim's pre-existing illnesses because he did not have access to medical documentation. The death occurred several months after surgery and was associated with numerous illnesses and complications, including pneumonia caused by inadequate lung ventilation during recovery. According to the expert in neurosurgery, mortality in cases of such cranio-cerebral injuries exceeds 80%. Although earlier surgical intervention increases the chances of survival, the likelihood of survival—and of complications leading to death—depends significantly on the patient's overall health condition. The victim had a documented history of psychiatric disorders, gastrointestinal surgery, and pulmonary inflammation, indicating a weakened immune system and a heightened

³⁴ Judgment of the County Court in Zagreb, Case No. KŽ-634/2021-7, 29 November 2022.

susceptibility to infection. The experts concluded that, given the victim's comorbidities and the time elapsed between injury and death, the fatal outcome could not be excluded even if he had been referred to surgery at the first examination and the injuries had been immediately diagnosed.³⁵

An analysis of this more recent case confirms that Croatian judicial practice is consistent in applying the theory of objective imputation in cases of negligent medical treatment, specifically through the concept of so-called lawful alternative conduct. The courts examine whether the same consequence would certainly have occurred even if the accused had acted with due care. It is noteworthy that legal scholars, including Novoselec, employ the standard of probability bordering on certainty, whereas judicial practice refers to complete certainty, which appears to represent an even higher standard of proof of causation required in criminal proceedings.

6. CONCLUSION

The full complexity of the problem of causation in criminal law is most clearly manifested in the offence of negligent medical treatment. Medicine is unique in that it represents a combination of natural sciences and the humanities, both of which are essential to its functioning.³⁶ From the natural-scientific perspective, the principal difficulty lies in the fact that it is impossible to know with one hundred per cent certainty what is true in any given research question, even though medical knowledge is grounded in such research.³⁷ Even in situations where relatively firm knowledge exists regarding the outcomes of specific medical procedures, a certain number of cases will almost invariably result in a negative outcome despite all appropriate medical measures having been undertaken. Such outcomes may occur even where the medical intervention was performed *lege artis*.

This natural-scientific "chaos," in which nothing can be determined with complete certainty, must nevertheless be subsumed under legal norms—specifically criminal law norms—which require strict determinacy, since their violation interferes with the highest legal values, such as personal liberty, as well as with

³⁵ Judgment of the Municipal Court in Zlatar, Case No. K-269/2020-30, 28 April 2021.

³⁶ Dreyfus H. L., *Medicine as Combining Natural and Human Science*, *The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine*, Volume 36, Issue 4, August 2011, p. 335.

³⁷ Ioannidis JPA, *Correction: Why Most Published Research Findings Are False*, *PLOS Medicine* 19(8), 2022.

the right to continue practising the medical profession as a legal consequence of conviction.

Legal theory applies to the offence of negligent medical treatment the theory of objective imputation, supplemented by the corrective of so-called lawful alternative conduct and the concept of hypothetical causality. However, this accepted theoretical model is itself practically limited by the very fact that it is impossible to determine with absolute certainty whether undertaken or omitted medical procedures would indeed have led to the deterioration of illness or impairment of health. This shortcoming is mitigated by establishing causation at the level of probability bordering on certainty.

An analysis of judicial practice demonstrates that Croatian courts align with the predominantly accepted legal theory by requiring a high degree of probability. It is noteworthy that legal theory employs the notion of probability bordering on certainty, whereas the most recent Croatian case law refers to complete certainty. It may therefore be concluded that Croatian judicial practice demands an even higher standard of certainty than that articulated in legal theory.

Such an approach is both correct and commendable. It is correct from the perspective of the principle *in dubio pro reo*, as it is impermissible to convict any person where there remains cognisable doubt that the consequence would have occurred irrespective of that person's conduct or omission. It is commendable because the offence of negligent medical treatment is a result-based offence requiring the realisation of a harmful consequence stemming from unprofessional conduct. If a lower degree of probability were accepted in linking negligent conduct to the consequence, there would be a risk that the offence of negligent medical treatment would approximate offences of endangerment, which would be unacceptable.

The positive aspect of this principled position in recent judicial practice lies in the fact that, in cases of the criminal offence of negligent medical treatment, only extreme instances of unprofessional medical conduct and omissions—those that with complete certainty result in the deterioration of illness or impairment of another person's health—are subject to criminal punishment. In this manner, human health is protected while medical professionals are enabled to practise their profession in a more relaxed and secure manner, free from the pressures of defensive medicine. They may do so in the knowledge that criminal liability arises only in cases of extreme professional misconduct that with complete certainty cause the prohibited harmful consequence.

REFERENCES

BOOKS AND ARTICLES

1. Cvitanović L., Derenčinović D. et al., *Kazneno pravo posebni dio*, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2018.
2. Dreyfus H. L., *Medicine as Combining Natural and Human Science*, The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine, Vol. 36, No. 4, August 2011, pp. 335–341.
3. Firkins G., *Rethinking Causation in English Criminal Law*, The Journal of Criminal Law, Vol. 87, No. 1, 2023, pp. 20–36.
4. Garačić A., *Kazneni zakon u sudskoj praksi*, Libertin naklada, Rijeka, 2023.
5. Ioannidis JPA, *Correction: Why Most Published Research Findings Are False*, PLOS Medicine, Vol. 19, No. 8, 2022.
6. Martinović I., *O kriteriju razlikovanja pravih i nepravih kaznenih djela nečinjenja*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 65, No. 1, 2015, pp. 127–149.
7. Martinović I., *Problem uzročnosti u kaznenom pravu*, Hrvatski ljetopis za kazneno pravo i praksu, Vol. 19, No. 1, 2012, pp. 77–105.
8. Mišić Radanović N., *Prijepori o kaznenoj odgovornosti medicinskih djelatnika za stručnu pogrešku*, Godišnjak Akademije pravnih znanosti Hrvatske, Vol. XI, No. 1, 2020, pp. 39–59.
9. Mišić Radanović N., Vukušić I., *Causation in medical malpractice*, EU and Comparative Law Issues and Challenges Series (ECLIC), Vol. 4, 2020, pp. 779–804.
10. Mišić Radanović N., Vukušić I., *Odnos različitih vrsta deliktne odgovornosti zdravstvenih radnika*, Zbornik radova s međunarodnog kongresa "2. Kongres KOKOZA i 4. Hrvatski kongres medicinskog prava s međunarodnim sudjelovanjem", Pravni fakultet Sveučilišta u Splitu, Split, 2020.
11. Miziara I. D., Miziara C. S. M. G., *Medical errors, medical negligence and defensive medicine: A narrative review*, Clinics, Universidade de Sao Paulo, Brazil, Vol. 77, 2022, pp. 1–7.
12. Mrčela M., Vuletić I., *Granice nehajne odgovornosti za kazneno djelo nesavjesnog liječenja*, Zbornik radova Pravnog fakulteta u Splitu, Vol. 54, No. 3, 2017, pp. 683–702.
13. Mrčela M., Vuletić I., *Liječnik i kazneno pravo*, Narodne novine, Zagreb, 2019.
14. Novoselec P., Bojanić I., *Opći dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2013.
15. Parenta I., *Temeljni problemi u primjeni pravila in dubio pro reo: doseg, trenutak primjene i odnos s drugim procesnim institutima*, Hrvatski ljetopis za kaznene znanosti i praksu, Vol. 30, No. 1, 2023, pp. 147–174.

16. Roksandić Vidlička S., *Aktualna pitanja pojedinih kaznenih djela protiv zdravlja ljudi*, Hrestomatija hrvatskog medicinskog prava, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2016, pp. 815–834.
17. Roksandić Vidlička S., Pražetina Kaleb R., *Utvrdjivanje pravnog kontinuiteta i tumačenje elemenata bića kaznenog djela nesavjesnog liječenja*, Zbornik radova s međunarodnog kongresa: "1. Kongres KoKoZ-a i 3. Hrvatski kongres medicinskog prava s međunarodnim sudjelovanjem", Pravni fakultet Sveučilišta u Splitu, Split, 2019, pp. 305–322.
18. Simester A., *Causation in (Criminal) Law*, Law Quarterly Review, Vol. 133, No. 3, 2017, pp. 416–441.
19. Vuletić I., *Medical Malpractice as a Separate Criminal Offense: a Higher Degree of Patient Protection or Merely a Sword Above the Doctors' Heads? The Example of the Croatian Legislative Model and the Experiences of its Implementation*, Medicine, Law & Society, Vol. 12, No. 2, October 2019, pp. 39–60.
20. Vukušić I., *Lex certa u poredbenom pravu*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 73, No. 1, 2023.
21. Vukušić I., *Uzročnost kod kaznenih djela nečinjenja*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 74, No. 2, 2024, pp. 405–431.

LEGAL ACTS

1. Criminal Code of the Republic of Croatia ("Official Gazette" br. 125/11., 144/12., 56/15., 61/15., 101/17., 118/18., 126/19., 84/21., 114/22., 114/23., 36/24, 136/25)

COURT PRACTICE

1. Judgment of the County Court in Bjelovar, Case No. Kž-443/2011-3, 26 February 2012
2. Judgment of the Municipal Court in Bjelovar, Case No. K-105/09-44, 14 September 2011
3. Judgment of the County Court in Zagreb, Case No. Kž-634/2021-7, 29 November 2022
4. Judgment of the Municipal Court in Zlatar, Case No. K-269/2020-30, 28 April 2021

UDK: 004.8 : 343.57 (439)

004.8 : 343.9 (439)

Preliminary communication

Henrietta Németh-Kiss, PhD student

Faculty of Law, University of Pécs, Hungary

E-mail: nemeth-kiss.henrietta@ajk.pte.hu

ORCID ID: 0009-0007-1421-7146

THE IMPACT OF DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE ON THE CRIMINAL LAW ASSESSMENT OF DRUG TRAFFICKING IN HUNGARY

ABSTRACT

This study examines the effects of digital transformation and artificial intelligence (AI) on drug trafficking. As a result of technological advancements, illegal markets have partially shifted from the physical to the virtual realm, where anonymity and automated processes dominate. The aim of the research is to analyze how technical innovations such as the darknet, cryptocurrencies, and AI-based solutions are reshaping traditional criminal behaviors. In addition to presenting technological trends, the study draws on an analysis of the drug-related provisions of the current Hungarian Criminal Code. Domestic case law is discussed, with particular regard to the Supreme Court's decision examining the connection between ordering drugs online and acquiring the right to dispose of them. The paper presents the Hungarian legislature's response to the emerging legal dilemma, namely the new criminal conduct introduced by the 2025 amendment. The paper offers a critical assessment of this solution, highlighting the limitations of the new approach's applicability in light of the specific characteristics of drug purchases on the dark web. In conclusion, a proposal is outlined that, rather than introducing new elements of the offense, advocates for a more modern interpretation of the existing conceptual framework, one adapted to the digital reality. The study contributes to a better understanding of the relationship between technological development and criminal law, aiding in the evaluation of the effectiveness of legislative responses.

Keywords: artificial intelligence, digitization, drug trafficking, Hungary, cybercrime

1. INTRODUCTION

In today's digital world, the online space is an integral part of our everyday lives, but this dependence does not stop at legal use; it also permeates the world of serious and organized crime. Today, almost all forms of organized crime are present in the digital space: whether it's online fraud, drugs, or money laundering, the internet has become a mainstay of the criminal world. Criminals are becoming increasingly professional in their use of digital infrastructure, with technology serving as both a tool for their activities and a shield against the authorities, as well as a specific target.¹ Artificial intelligence and new technologies are accelerating crime and opening up entirely new opportunities for criminal networks. These developments are taking crime to a new level: it is becoming faster and more efficient, and authorities must keep up in an increasingly complex and rapidly changing world.²

The effects of technological advances are also clearly evident in the drug market, with innovations in various areas becoming the main aids to criminal networks throughout the entire drug supply chain. This is also evident in new methods of drug production, which enable higher yields, preparations with higher active ingredient content or purity, and novel consumer products. At the same time, developments in the digital world are also playing into their hands, as can be seen in the constant renewal of online drug distribution.³

Numerous national and global online platforms are now used to conduct drug sales, which are popular with both sellers and buyers due to their quick access and anonymity. At the retail level, open websites, including legal web shops and social media, are used to sell new psychoactive substances, counterfeit medicines and, to a lesser extent, traditional illicit drugs. Open websites are also used to purchase drug precursors and other chemicals needed for manufacturing. Current data indicate that retail distribution is increasingly moving to social media and various applications, ranging from public profiles to private messages and closed forums. Sales are also facilitated by darknet sites, which use encryption and cryptocurrency payments to ensure anonymity, serving customers worldwide or even targeting specific countries or language groups.⁴

¹ Europol, *The changing DNA of serious and organised crime*, European Union serious and organised crime threat assessment, 2025, p. 16.

² Europol, *The changing DNA of serious and organised crime*, European Union serious and organised crime threat assessment, 2025, p. 6.

³ EUDA, *EU Drug Market: Drivers and facilitators — Technology and innovation*, 2024, p. 3.

⁴ European Drug report 2025 Trends and developments, 2025, pp. 14-15.

Technological-based restructuring has partially shifted the scene of crime from the physical world to virtual space, where anonymity and automated processes dominate. According to Judith Aldridge, the traditional, violence-based structure of online drug trafficking has been replaced by a decentralized structure based on trust scores and encrypted logistics.⁵

In this situation, legislators and law enforcement agencies must find new answers when assessing drug-related crimes under criminal law.

2. THE ROLE OF THE DARKNET AND CRYPTOCURRENCIES IN ONLINE DRUG TRAFFICKING

Darknet drug transactions represent a new form of drug trafficking in the sense that they are reshaping local "offline" markets and functioning as a new channel for drugs.⁶ The darknet trade in illegal goods has undergone tremendous growth in recent years: a global industry has grown up that mimics the structure of legal platforms such as eBay or Amazon, with products advertised with photos and descriptions, the darknet community rating the reliability of traders, and 24-hour customer service available.⁷

To understand this phenomenon, it is essential to clarify the structure of virtual space, as a significant portion of online activities take place in layers that are invisible to everyday users.

2.1. Layers of the Internet

The internet basically consists of two parts: the surface web (clearnet) and the deep web. The surface web is the layer of the internet that is accessible to anyone: the websites found here and their content can be found using traditional browsers, such as Google Chrome, and have typical domain endings, such as .com. In contrast, the deep web makes up a much larger part of the internet. It is accessible with any browser, but its content cannot be displayed by traditional search engines and can therefore only be viewed by a small group of users. This may be because

⁵ Aldridge, J.; Décary-Héту, D., *Not an 'eBay for Drugs': The Cryptomarket "Silk Road" As a Paradigm Shifting Criminal Innovation*, 2014, p. 2.

⁶ Aldridge, J.; Décary-Héту D., *Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets*, International Journal of Drug Policy, 35/2016, p. 8.

⁷ Vogt S., *Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus“ der Kriminellen?*, Die Kriminalpolizei, 2/2017, p. 5.

it consists of intranets accessible to specific closed user groups or content with a paywall function.⁸

The darknet can be defined as a small segment of the deep web that hides the user's location and identity, thus ensuring anonymity. Special software, such as Tor, and the appropriate settings are required to access dark web sites.⁹ The concept of the dark web is usually associated with crime, but researchers prefer to use a neutral definition and refer to the darknet only as a means of access (anonymizing software), which says nothing about the legal status of its content.¹⁰

Tor (The Onion Router) is therefore anonymity software that encrypts IP addresses or domain names, thereby preventing communication from being traced back to the parties involved.¹¹ Its developer compared the structure of Tor technology to an onion, whose center is hidden under layers of skin. The same can be observed with Tor: the identity and activities of a given user are protected by multiple layers of anonymization. The technology is based on the multiple transmission of data traffic.¹² The Tor browser is similar to a standard web browser, with the difference that Tor connects the user to the internet via the Tor network. When using Tor, internet traffic is randomly routed through a network of servers before reaching its final destination. In addition to Tor, there are several other encryption software programs available, such as I2P and Freenet, but Tor is currently the most popular.¹³

After installing the Tor software and configuring the appropriate settings, the Tor browser connects to the Tor network, which ensures anonymity. Traditional browsers are not suitable for searching; special search engines are required that are specifically designed for use with darknet sites, enabling them to find hidden content. The most commonly used darknet search engines include Torch, DuckDuckGo, and HiddenWiki.¹⁴

⁸ May, S., „Tor” in eine andere Welt? Begriffe, Technologien und Widersprüche des Darknets, Aus Politik und Zeitgeschichte. Darknet, 46–47/2017, p. 4.

⁹ Was ist eigentlich das Darknet? <https://blog.gdata.de/2026/01/38350-was-ist-eigentlich-das-darknet>, 12 December, 2025.

¹⁰ Tzanetakis, M., *Digitalisierung von illegalen Märkten. Folgen, Grenzen und Perspektiven*. In: Feustel, R.; Bröckling, U.; Schmidt-Semisch H. (Eds.), *Handbuch Drogen in sozial- und kulturwissenschaftlicher Perspekt*, Springer VS, Wiesbaden 2019, p. 479.

¹¹ Tzanetakis, M., *Zur globalen Ökonomie von digitalen Drogenmärkten*. In: Rausch. *Wiener Zeitschrift für Suchttherapie*, 2017, p. 192.

¹² May, *op. cit.* note 8, p. 5.

¹³ Serbakov, M., *Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem*, Büntetőjogi Szemle, 1/2020, pp. 92-93.

¹⁴ Bergmann, J., *Darknet Suchmaschinen*, 2021, <https://digital-hacks.de/darknet-suchmaschinen/>, 6 October, 2025.

2.2. How do illegal drug markets operate on the dark web?

Access to illegal darknet markets is usually subject to various conditions: on some sites, new traders can only be accepted if they are deemed trustworthy by existing traders. Often, new buyers must also be approved by the operator and pay a membership fee.¹⁵

The rating system helps buyers choose the right offer and dealer. Following the example of legal markets, a feedback system has also been developed on darknet sites, where buyers can rate the reliability of dealers: they can provide feedback on, among other things, the quantity and quality of the drugs ordered, customer service, and communication with sellers.¹⁶

Blockchain technology and cryptocurrencies ensure that money movements are concealed, eliminating the central banking system from the process. On illegal cryptocurrency markets, goods are paid for with virtual currencies, the best known of which is Bitcoin. However, due to the developing analytical methods of the authorities, criminals are increasingly turning to currencies that offer true anonymity, such as Monero.¹⁷ Parties can generally choose from three different payment systems. One variation is when the buyer first pays the cryptocurrency into an escrow account and the payment to the merchant is approved when the buyer confirms receipt of the goods. The advantage of this payment mechanism is that it protects buyers from potential fraud by merchants, but it also carries the risk that the escrow account manager will abuse their position (exit scam). It is also possible for the money to be transferred to the merchant before the goods are shipped, which carries the obvious risk that the goods will not be shipped. The third payment option – which is the most secure, but also the most technically complex and therefore rarely used – is when at least two of the three parties involved (the market operator, the trader, and the buyer) must confirm the transaction for the payment to be approved (Multisig).¹⁸

Drugs are most often delivered by mail or courier services, although in certain regions, such as Hydra Market, delivery via physical hiding places (so-called "dead drops") is also common. Safe and clean packaging of drugs is important in order to avoid detection. For this reason, many dealers maintain a separate room for preparing drugs, thereby avoiding leaving DNA traces or drug residues on the

¹⁵ Was ist eigentlich das Darknet? <https://blog.gdata.de/2026/01/38350-was-ist-eigentlich-das-darknet>, 12 December, 2025.

¹⁶ Europol, *Drugs and the darknet Perspectives for enforcement, research and policy*, 2017, p. 27.

¹⁷ Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2021, p. 9.

¹⁸ Tzanetakakis, M. *op. cit.* note 10, p. 485.

packaging. Packages are delivered in various ways: some buyers rent a separate mailbox for delivery, others use false information to obtain the delivery address of others, and still others provide their own name and address. Various guides are also available on darknet forums to inform buyers about safe delivery.¹⁹

Despite the fact that the better-known crypto markets – Silk Road, Dream Market, Hydra Market – have been operating for several years, it can be said that illegal darknet sites are short-lived, usually active for around eight months.²⁰ The market may be closed to the detriment of users: the operator suddenly shuts down the site without completing transactions and payments. However, it sometimes happens that the site operator announces the closure of the market in advance, but successful intervention by law enforcement agencies or hacker attacks can also lead to the site being shut down.²¹

2.3. Why do consumers choose the darknet?

In their study, Barrat, Ferris, and Winstock examine, among other things, the reasons why consumers decided to order drugs from Silk Road.²² In the countries surveyed, respondents cited four main reasons in the same order: the wide selection of drugs, their higher quality, the convenience of online purchasing, and positive reviews of the dealers. Other relevant factors included anonymity, lower drug prices, the absence of physical contact with dealers, and the lack of a social network.²³

In this context, the anonymity of transactions deserves a brief mention. Due to various encryption software and payment with cryptocurrency, the identity and location of the dealer and the buyer remain hidden. This anonymity provides two-way protection: it protects users from law enforcement agencies, and the identities of the participants remain hidden from each other. Since traders and buyers only know each other's usernames, it is completely impossible for them to identify each

¹⁹ Afilipoaie, A.; Shortis, P., *From Dealer to Doorstep – How Drugs Are Sold On the Dark Net*, 2015, p. 4.

²⁰ UNODC, *World Drug Report*, 2021, p. 75.

²¹ Europol, *Drugs and the darknet Perspectives for enforcement, research and policy*, 2017, p. 16.

²² During the research, darknet users from Australia, the US, and the UK answered the questions.

²³ Barrat, M.; Ferris, J.; Winstock, A., *Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States*, 2014.

other. For this reason, darknet users feel much safer than those involved in street drug trafficking.²⁴

It should also be noted that the drugs and psychoactive substances available on the darknet are of higher quality than those available through traditional drug trafficking. The higher quality of the drugs was confirmed by an anonymous survey: 72-77% of respondents said that the drugs ordered on Silk Road were of better quality than those available through offline trade.²⁵ When consumers have to choose drugs from the range offered by street dealers, they are buying substances that have passed through numerous intermediaries in the traditional market before reaching the dealer. At these stations, the quantity of drugs arriving at the resellers is further increased by dilution or enrichment for additional profit, thereby reducing their quality.²⁶ There is no guarantee of the quality of drugs offered on the crypto markets, but online drug markets have features that encourage dealers to offer the best possible quality, including the aforementioned payment and feedback system and positive customer reviews.²⁷

Another disadvantage of offline drug trafficking is its geographical limitation: drugs reach consumers via several countries, stations, and individuals. From the traffickers' point of view, this makes it difficult to control the activities of more distant intermediaries and increases the risk of detection due to the cross-border transport of drugs. In addition, dealers and consumers are geographically limited, so the availability of drugs and psychoactive substances varies. It is quite possible that the drug the buyer wants to purchase is out of stock, in which case the buyer must either wait for the next shipment or find another dealer. In contrast, online drug markets are not affected by geographical constraints, so they offer consumers a wider selection of drugs and easier access compared to the physical drug trade.²⁸

The lack of physical contact brings with it an additional factor: non-violence. Offline drug trafficking involves numerous conflicts, which can easily lead to violence. Of course, disagreements also arise in anonymous drug markets, e.g. if the buyer does not receive the expected quality or quantity of drugs, or if the shipment does not arrive.²⁹ However, the absence of physical encounters reduces

²⁴ Kiss, T., *Miért népszerű a darknetes kábítószer-kereskedelem?*, In: Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére. Navigare necesse est, Ludovika Egyetemi Kiadó, Budapest 2021, p. 270.

²⁵ Tzanetakis, M. *op. cit.* note 11, p. 193.

²⁶ Kiss, *op. cit.* note 31, pp. 271-272.

²⁷ Aldridge, J.; Décary-Héту, D., *Cryptomarkets: The Darknet As An Online Drug Market Innovation. Final report to NESTA*, 2015, p. 22.

²⁸ Tzanetakis, M. *op. cit.* note 10, p. 483.

²⁹ Tzanetakis, M. *op. cit.* note 11, p. 193.

the number of violent acts usually associated with drug trafficking. According to the practice established on crypto markets, the parties can resolve problematic situations directly with each other, but they can also involve the administrator. They also have the option of discussing the conflict with other users in various forums, and an automatic feedback system is also available to them.³⁰

The higher consumer price of drugs and psychoactive substances available on the street is another disadvantage related to distance. While in traditional drug trafficking, the price of drugs increases at each stage and with each additional activity (e.g., drug storage, smuggling) increases the price of drugs, anonymous platforms offer a wide range of drugs at more favorable prices to consumers by eliminating most of the stations and intermediaries.³¹

Finally, it should be noted that the online drug market directly connects consumers and distributors. Traditional drug procurement is based on personal connections and social capital. If the buyer's extensive network of contacts does not include individuals involved in drug distribution, the transaction cannot take place. Even if there are such individuals, the dealer's access to specific substances is severely limited. In contrast, online drug markets provide an opportunity to obtain special, harder-to-find substances without personal connections.³²

2.4. Algorithms and artificial intelligence in the drug market

Artificial intelligence (AI) is not just a new technical tool, but a technology that fundamentally changes the methods of crime. According to Glaser, AI creates opportunities that did not exist before. This does not necessarily mean completely new types of crime, but rather that traditional methods of crime are being transformed by it.³³ According to forecasts for the future, by 2035, unmanned systems—such as drones and self-driving vehicles—will become everyday tools of organized crime.³⁴

This technological development is having an impact not only on drug trafficking, but also on the very first stages of production. Innovations in the use of raw

³⁰ Morselli, C.; Décary-Héту, D.; Paquet-Clouston, M.; Aldridge, J., *Conflict Management in Illicit Drug Cryptomarkets*, 2017, p. 7.

³¹ Kiss, *op. cit.* note 31, p. 272.

³² Dési, Á., *A digitális bennszülött generáció és a kábítószer tudatosság*, Kriminológiai Közlemények, 78, 2018, p. 96.

³³ Glaser, S., *Künstliche Intelligenz im Strafrecht*, SIAK-Journal, 1/2024, p. 11.

³⁴ Europol, *The Unmanned Future(s) The impact of robotics and unmanned systems on law enforcement*, 2025, p. 41.

materials are fundamentally transforming the manufacture of synthetic drugs. In Europe, manufacturers have switched from strictly controlled precursors to freely available chemicals from which the necessary raw materials can be easily extracted or from which various drugs can be produced directly. This also demonstrates that drug manufacturers are becoming increasingly adept at adopting methods used in the pharmaceutical industry to avoid detection. In this area, the use of artificial intelligence—such as chatbots—to discover new compounds and molecules that can be used in the production of illegal drugs could pose a major threat in the future.³⁵

However, the rise of this technology goes beyond chemical innovation; it also fundamentally changes the relationship between the dealer and the buyer by eliminating direct human contact. The use of generative AI and automated chatbots in interactions between the "dealer" and the "buyer" eliminates direct human contact.

The continuous development of darknet markets and their convergence with social media and open web applications has made the work of investigators and authorities even more difficult. For example, in 2021, a "shop bot" called Televend appeared, operating through the Telegram messaging app and backed by an encrypted Tor-based interface. After buyers added Televend as a contact on Telegram and performed a few simple steps, they could access a list of drug dealers. The store was operated by a bot 24 hours a day, handling orders and all administrative functions. This solution provided protection for sellers and prevented the risk of distributed denial-of-service (DDoS) attacks. Although Televend was shut down in the fall of 2021, the system demonstrated that the method of linking darknet markets and messaging apps in drug trafficking works very well. Due to the convenience and greater security it offers users, as well as the protection it provides to sellers, it is possible that this method will reappear in the future, or may even be in use already.³⁶

It is also important to note that AI offers law enforcement new opportunities in the fight against drug trafficking. Algorithms are capable of analyzing billions of data points in real time, allowing investigators to connect clues found on the dark web with data available on the public internet. This enables authorities to not only

³⁵ EUDA, EU Drug Market: Drivers and facilitators — Technology and innovation, 2024, p. 4.

³⁶ EUDA, EU Drug Market: Drivers and facilitators — Technology and innovation, 2024, p. 12.

apprehend couriers, but also identify the actual leaders of criminal organizations based on their digital footprints.³⁷

AI is therefore simultaneously transforming the methods of crime and making detection in the digital world more effective.

3. THE LEGAL ELEMENTS OF DRUG TRAFFICKING AND DRUG POSSESSION IN THE HUNGARIAN CRIMINAL CODE

The Hungarian Criminal Code classifies drug-related criminal offenses according to whether they are related to drug distribution or consumption. Drug trafficking offenses include offering, transferring, distributing, and trading drugs, as well as providing the material resources necessary to commit the crime.

The legislator regulates the so-called consumer or purchaser type of criminal conduct in the legal definition of drug possession. The cultivation, production, acquisition, possession, importation into the country, exportation from the country, transportation within the country, and provision of material resources for these acts are punishable. "With regard to possession, it should be emphasized that it is only mentioned in the name of the criminal offense; the criminal acts must be interpreted independently and in relation to each other, and actual possession can only be relevant in relation to individual acts."³⁸

The Hungarian Criminal Code does not define what acts fall under the concept of criminal conduct, but Opinion 57 BK and Decision 1/2007 BJE contain guiding principles in this regard. Since this study focuses on the digital dimension of drug trafficking, the scope of the crimes examined has been narrowed in the legal analysis. This section of the study focuses on behaviors that can be digitally transmitted or linked to online transactions (trafficking, offering, acquisition), logically excluding forms that are typically tied to a physical location, such as cultivation or production.

³⁷ Voyager Labs: *Artificial Intelligence and the Fight Against Illegal Narcotics*, 2021, <https://www.voyager-labs.com/artificial-intelligence-and-the-fight-against-illegal-narcotics/>, 3 December, 2025.

³⁸ Szomora Zs., *Mi köze a kábítószer birtoklása büntetnének a Polgári Törvénykönyvhöz? Avagy hogyan ne értelmezzünk büntetőtényállást*, In: Tanulmányok Dr. Balogh Ágnes egyetemi docens tiszteletére, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs 2023, p. 119.

3.1. Drug trafficking

In the legal definition of drug trafficking, regulated supply refers to soliciting another person to receive drugs, which constitutes a criminal offense if the solicitation is unsuccessful; otherwise, another criminal offense is established (transfer, distribution, or trafficking).³⁹

If, as a result of the offer, the recipient accepts or acquires the drugs, the person supplying the drugs has carried out the transfer of the drugs. The transfer therefore means the transfer of possession of the drugs, while the acquisition of the drugs means taking possession of them. The act of the perpetrator is considered to be the transfer of drugs if it is done to a specific person; if the perpetrator transfers the drugs to more than one person, their act corresponds to the distribution of drugs or drug trafficking.⁴⁰

Distribution occurs when the perpetrator supplies the drug, either free of charge or in exchange for payment, to several or an indeterminate number of persons. This criminal conduct may also occur when the perpetrator is in direct contact with only one person (to whom he or she hands over the drugs), but not with the sole intention of the recipient consuming the drugs himself or herself, but with the intention of passing them on to another person or other persons.⁴¹

Trafficking is carried out by anyone who participates in the distribution of narcotics with the aim of making a profit. Trafficking is a broader offense than distribution: it encompasses all activities that facilitate the delivery of drugs to dealers or consumers, such as the packaging, storage, transport, and distribution of drugs.⁴²

Both placing on the market and trading necessarily involve transfer, but cannot be narrowed down to actual transfer. The latter occurs when the transfer of drugs is made solely for the purpose of consumption by the recipient. The transfer that necessarily accompanies placing on the market, as well as trafficking, may consist of several sub-activities prior to this.⁴³ It may include finding sellers or buyers, using intermediaries, preliminary discussions, purchasing, viewing and examining

³⁹ Opinion No. 57 of the Criminal Law Department of the Supreme Court on the criminal liability for drug trafficking and drug possession

⁴⁰ Opinion No. 57 of the Criminal Law Department of the Supreme Court on the criminal liability for drug trafficking and drug possession

⁴¹ Opinion No. 57 of the Criminal Law Department of the Supreme Court on the criminal liability for drug trafficking and drug possession

⁴² *Ibid.*

⁴³ Supreme Court Decision BH 2002.299, Supreme Court Decision BH 2002.175

the goods, concluding the agreement, storing, transporting and dispensing the goods, preliminary reconnaissance of the place of transfer, securing means of transport and escorts, etc. it therefore covers all activities aimed at placing the drugs on the market, even through additional intermediaries.⁴⁴

3.2. Drug possession

Acquiring drugs means taking possession of them, which may be done by agreement with the previous owner (free of charge or in return for payment), but also without such an agreement. Thus, acquisition includes finding, purchasing, accepting without consideration, but also taking possession through theft or robbery. From the point of view of the commission of the crime, it is irrelevant whether the perpetrator takes possession of the drugs for himself or for another person. The crime is completed when the state of possession changes, and there is no need for the drug to be held in possession for a longer period of time. The acquisition of a drug is often not followed by longer-term possession, i.e., holding, because the acquirer consumes or uses it immediately.⁴⁵

However, the acquisition of drugs for the purpose of trafficking in itself falls within the scope of trafficking, and therefore the perpetrator who commits this act commits the completed crime of drug trafficking.⁴⁶

Transit-type criminal conduct (importing drugs into the country, exporting them from the country, or transporting them within the country) can only be established in the case of perpetrators who physically move the object of the offense for their own use or to satisfy their own needs. If the transport activity serves to deliver the drugs to another person or persons, this constitutes a sub-activity related to distribution, and thus constitutes transfer, placing on the market or trade.⁴⁷

4. CRIMINAL BEHAVIOR IN CYBERSPACE: POSSIBLE QUESTIONS OF INTERPRETATION

The dogmatic system of Hungarian criminal law is fundamentally based on acts committed in the physical world. However, when drug trafficking takes place on

⁴⁴ *Ibid.*

⁴⁵ Supreme Court Decision Bfv.1010/2021/6

⁴⁶ Supreme Court Decision BH 2017.5.144

⁴⁷ Beregszászi G., *Az egészséget veszélyeztető bűncselekmények*, In: Belovics, E.; Polt, P., A Büntető Törvénykönyv kommentárja, ORAC Kiadó, Budapest 2023.

the internet, the interpretation of the criminal acts defined in Sections 176–178 of the Criminal Code may raise dogmatic questions, so we need to consider what these concepts mean in the digital environment.

The concept of offering is relatively easy to define in the online space. If the seller uses an AI-based chatbot to negotiate with the buyer, the criminal act of "offering" is already committed by making an offer on the digital platform, regardless of whether the parties communicated directly with each other.

However, the concept of transfer requires a specific interpretation, as according to Hungarian judicial practice, transfer means the handing over of drugs from one person to another. In a digital environment, however, there is no physical contact between the perpetrator and the buyer. It is therefore questionable whether the "transfer" is completed when the drugs are posted or only when the buyer actually takes possession of them (e.g., at a "dead drop" point), where instructions are sent to the user by an algorithm.

The interpretation of distribution is also broadening in the range of criminal conduct, as its essence is that the drug becomes accessible to several people. Darknet markets and AI-controlled distribution systems perform precisely this function.

This statement also applies to the conduct of trading. Since the essence of trading is profit-making and regularity, automatic tasks performed by software—such as inventory control, continuous price adjustment, or customer review management—become part of the trader's work and can be evaluated as sub-actions. In this situation, the code and operation of the program reveal the perpetrator's intent: he uses technology to control sales. Thus, for the sake of profit, he is constantly present on the illegal market, even if he is not physically there himself.

When it comes to drug possession, interpreting the point of acquisition can be tricky if the drugs were ordered online. It often happens that a buyer orders drugs on the internet but never receives them because, for example, the authorities seize the package in the meantime. In such cases, it must be examined whether placing the order alone establishes the right to dispose of the drugs, i.e., whether the buyer who never physically received the substance can be punished.

To answer this question, it is worth examining domestic legal practice, as Hungarian courts have already heard a case that dealt with precisely this dilemma.

In the case on which the decision⁴⁸ was based, the perpetrator ordered a basic quantity of cannabis from abroad. The drugs arrived in Hungary as a letter sent by Magyar Posta Zrt. Nemzetközi Posta Kicszerelő Központ (Hungarian Post International Mail Exchange Center), addressed to the perpetrator. The authorities seized the drugs at the airport before they were delivered.

While the court of second instance found that the act constituted the criminal offense of possession of drugs imported into the country, the Supreme Court classified the act as acquisition of drugs.

In its reasoning, the Supreme Court pointed out, first and foremost, that the persons involved in the delivery were mistaken in importing the drugs into Hungary.

Since the perpetrator did not come into physical contact with the drugs seized at the airport, he was unable to transport them to Hungary. The perpetrator's goal was to obtain the drugs, which, in the opinion of the Supreme Court, was achieved by establishing the right to dispose of the drugs.

In its decision, the Supreme Court also referred to a case where the perpetrator transported drugs purchased abroad and thus acquired to Hungary. In this case, the correct classification of the act is possession of drugs committed by acquisition, because "acquisition provides earlier criminal law protection than importation into the country, since the territorial scope of the Criminal Code also covers conduct committed by Hungarian citizens abroad that constitutes possession of narcotics under Hungarian law, i.e., the acquisition of narcotics. Therefore, while in this case the acquisition of the drugs takes place abroad, the criminal act of "importation into the country" does not even enter the attempt stage before crossing the Hungarian border. The classification of the completed crime as acquisition is not affected if the perpetrator also engages in further criminal conduct involving the importation of the same drugs into the country.

However, the criminal law assessment of the act is different when "the perpetrator obtains the right of disposal over drugs that are physically located abroad without actually taking possession of them, and enlists the help of a third party to establish possession of the drugs. This is a typical form of cross-border drug trafficking, which is only relevant to the case under consideration insofar as it clearly illustrates that the right of disposal over drugs can be separated from possession. In such cases, acquisition is not linked to the person in possession, but to the right

⁴⁸ Supreme Court Decision BH 2023.4.89

of disposal: in the situation described, it is clear that the drugs are not acquired by the courier, but by the dealer who gives the courier instructions and has control over the drugs.

The same legal assessment applies to cases where drugs purchased abroad by an agent are not intended for distribution. In such cases, the principal is responsible for the acquisition of the drugs and the agent is responsible for importing them into the country.

In contrast, in the case under review, the perpetrator purchased the drugs from an unknown person abroad, in accordance with the rules governing contracts between absent parties in civil law. On the basis of these provisions, the Supreme Court concluded that by placing the order, the perpetrator acquired ownership of the drugs – the right to dispose of them – when they were posted abroad, regardless of the fact that the shipment did not come into his physical possession due to its seizure. "The right of disposal is typically, but not exclusively, associated with the possession of the drugs, i.e., the perpetrator acquires the drugs even without actual possession if he or she has the power to determine their destination."

Although the Supreme Court put an end to the case by applying civil law rules, the decision did not provide a satisfactory solution, so legislative intervention was ultimately necessary. In response, Hungarian lawmakers finally settled the debate with the 2025 amendment to the law by including a new criminal offense in the statute: ordering drugs for importation into the country.

In my opinion, the applicability of the new criminal offense may encounter serious obstacles in practice due to its specific nature. Since the legislator expressly stipulates that orders placed "for the purpose of importing into the country" are punishable, it is essential for the facts of the case that the perpetrator was aware of the foreign origin of the drugs at the time of placing the order. This subjective condition is particularly problematic in the case of purchases on the dark web: on anonymous platforms, the buyer orders from an unknown seller and has no information about the actual physical location of the drug or the place of dispatch. If the perpetrator cannot prove that the drugs will come from abroad, this new twist will not be applicable due to lack of intent.

5. CONCLUSION

The processes presented in the study highlight that the cyber dimension of drug trafficking and the use of artificial intelligence are no longer a distant future, but a

present reality. This puts the dogmatic framework of Hungarian substantive criminal law to the test and necessitates a refinement of legal interpretation.

In conclusion, it can be said that technological development does not stop at the gates of the legal system. While keeping in mind the principles of legal certainty and proportionality, Hungarian criminal law must be able to provide meaningful responses to the online forms of drug trafficking. The use of automated processes and algorithms allows transactions to take place without human interaction. This distance makes it difficult to interpret classic criminal behavior.

In my opinion, the previous criminal acts defined in the Criminal Code already covered all relevant acts related to drugs. Instead of specifically mentioning "ordering," a more effective solution would be to interpret the existing conceptual framework in a more modern way. Instead of adding new criminal acts, the emphasis should be placed on filling existing concepts with content. The 1/2007. BJE decision, which is still referred to today in the interpretation of drug-related crimes, was issued under the previous Criminal Code. Nearly two decades have passed since then, and due to the technological explosion (darknet, cryptocurrencies, AI) and the change in approach in the 2012 Criminal Code, this guideline has now become obsolete. I therefore consider it necessary to adopt a uniformity decision that contains a flexible interpretation of the existing framework, adapted to the digital world, which is capable of providing a meaningful response to 21st-century forms of crime.

REFERENCES

BOOKS AND ARTICLES

1. Afilipoaie, A.; Shortis, P., *From Dealer to Doorstep – How Drugs Are Sold On the Dark Net*, 2015, p. 4.
2. Aldridge, J.; Décary-Héту D., *Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets*, International Journal of Drug Policy, 35/2016, p. 8.
3. Aldridge, J.; Décary-Héту, D., *Cryptomarkets: The Darknet As An Online Drug Market Innovation. Final report to NESTA*, 2015, p. 22.
4. Aldridge, J.; Décary-Héту, D., *Not an 'eBay for Drugs': The Cryptomarket "Silk Road" As a Paradigm Shifting Criminal Innovation*, 2014, p. 2.
5. Barrat, M.; Ferris, J.; Winstock, A., *Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States*, 2014.

6. Beregszászi G., *Az egészséget veszélyeztető bűncselekmények*, In: Belovics, E.; Polt, P., *A Büntető Törvénykönyv kommentárja*, ORAC Kiadó, Budapest 2023.
7. Dési, Á., *A digitális bennszülött generáció és a kábítószer tudatosság*, *Kriminológiai Közlemények*, 78, 2018, p. 96.
8. EUDA, *EU Drug Market: Drivers and facilitators — Technology and innovation*, 2024, p. 3.
9. *European Drug report 2025 Trends and developments*, 2025, pp. 14-15.
10. Europol, *Drugs and the darknet Perspectives for enforcement, research and policy*, 2017, p. 27.
11. Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2021, p. 9.
12. Europol, *The changing DNA of serious and organised crime*, *European Union serious and organised crime threat assessment*, 2025, p. 16.
13. Europol, *The Unmanned Future(s) The impact of robotics and unmanned systems on law enforcement*, 2025, p. 41.
14. Glaser, S., *Künstliche Intelligenz im Strafrecht*, *SIAC-Journal*, 1/2024, p. 11.
15. Kiss, T., *Miért népszerű a darknetes kábítószer-kereskedelem?*, In: Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére. *Navigare necesse est*, *Ludovika Egyetemi Kiadó*, Budapest 2021, p. 270.
16. May, S., „Tor” in eine andere Welt? *Begriffe, Technologien und Widersprüche des Darknets*, *Aus Politik und Zeitgeschichte. Darknet*, 46–47/2017, p. 4.
17. Morselli, C.; Décary-Héту, D.; Paquet-Clouston, M.; Aldridge, J., *Conflict Management in Illicit Drug Cryptomarkets*, 2017, p. 7.
18. Serbakov, M., *Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem*, *Büntetőjogi Szemle*, 1/2020, pp. 92-93.
19. Szomora Zs., *Mi köze a kábítószer birtoklása büntetnének a Polgári Törvénykönyvhöz? Avagy hogyan ne értelmezzünk büntetőtényállást*, In: *Tanulmányok Dr. Balogh Ágnes egyetemi docens tiszteletére*, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs 2023, p. 119.
20. Tzanetakis M., *Digitalisierung von illegalen Märkten. Folgen, Grenzen und Perspektiven*. In: Feustel, R.; Bröckling, U.; Schmidt-Semisch H. (Eds.), *Handbuch Drogen in sozial- und kulturwissenschaftlicher Perspekt*, Springer VS, Wiesbaden 2019, p. 479.
21. Tzanetakis, M., *Zur globalen Ökonomie von digitalen Drogenmärkten*. In: *Rausch. Wiener Zeitschrift für Suchttherapie*, 2017, p. 192.
22. UNODC, *World Drug Report*, 2021, p. 75.
23. Vogt S., *Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus“ der Kriminellen?*, *Die Kriminalpolizei*, 2/2017, p. 5.

LEGAL ACTS

1. Act C of 2012 on the Hungarian Criminal Code, Hungarian Gazette, No. 92/2012.
2. Act XIX of 2025 on amendments to laws relating to the prohibition of the production, use, distribution, and promotion of narcotics, Hungarian Gazette, No. 55/2025.
3. Opinion No. 57 of the Criminal Law Department of the Supreme Court on the criminal liability for drug trafficking and drug possession
4. Supreme Court Decision 1/2007 on Criminal Law Uniformity in Matters of Drug-Related Crimes
5. Supreme Court Decision Bfv.1010/2021/6.
6. Supreme Court Decision BH 2002.175
7. Supreme Court Decision BH 2002.299
8. Supreme Court Decision BH 2017.5.144
9. Supreme Court Decision BH 2023.4.89

NETWORK RESOURCES

1. Bergmann, J., *Darknet Suchmaschinen*, 2021, <https://digital-hacks.de/darknet-suchmaschinen/>, 6 October, 2025.
2. Voyager Labs: *Artificial Intelligence and the Fight Against Illegal Narcotics*, 2021, <https://www.voyager-labs.com/artificial-intelligence-and-the-fight-against-illegal-narcotics/>, 3 December, 2025.
3. Was ist eigentlich das Darknet? <https://blog.gdata.de/2026/01/38350-was-ist-eigentlich-das-darknet>, 12 December, 2025.

UDK: 347.6 (4-67 EU)
342.7-053.2 (4-67 EU)
347.63-055.62 (4-67 EU)
Preliminary communication

Nikolina Tomaš, PhD student

Faculty of Law, University of Split, Croatia

E-mail: nikolina.tomas@pravst.hr

ORCID-ID: 0009-0002-8460-9448

FUNCTIONAL APPROACH TO THE RECOGNITION OF FAMILY RELATIONSHIPS IN THE CASE LAW OF EUROPEAN COURTS

ABSTRACT

*Although member states traditionally enjoy broad autonomy in the field of family law, the development of European case law has gradually led to a reassessment of the limits of that autonomy in cross-border situations. This is particularly evident in the context of recognising the legal effects of family relationships established in other member states. The paper proceeds from the research hypothesis that a functional approach to recognition has gradually emerged in European case law, allowing a distinction between the non-recognition of a family law institution as such and the obligation to recognise its legal effects where this is necessary for the protection of fundamental rights. Early elements of this approach can be identified in the case law of the European Court of Human Rights, particularly in *Mennesson and Labassee*, while the judgments of the Court of Justice of the European Union in *Coman* and *Pancharevo*, as well as more recent case law, have further elaborated this approach within the framework of EU law. It examines the development of this approach in the case law of the two European courts and the extent to which it can be regarded as a common methodological framework in cross-border family situations, particularly in cases concerning surrogacy and the free movement of European Union citizens. The central research question of the paper is whether this functional approach can be identified as a coherent methodological framework in the case law of European courts. The paper also briefly considers its relationship with the concept of the attenuated effect of public policy. The paper argues that the functional approach may be understood as a doctrinal tool that reconciles the protection of fundamental rights with the regulatory autonomy of member states.*

Keywords: *functional approach to the recognition, surrogacy, children's rights, family law*

1. INTRODUCTION

The normative regulation of family law has traditionally fallen within the sphere of broad state autonomy.¹ At the level of the European Union, harmonisation has primarily developed through private international law, particularly in the fields of jurisdiction, applicable law, and the recognition and enforcement of decisions, rather than through the unification of substantive family law.² As a result, significant differences persist between national legal systems, especially in relation to parenthood, the recognition of family relationships, and personal status.³ These differences acquire particular legal relevance in cross-border situations, where family relationships established in one member state seek to produce legal effects in another.⁴ The increasing mobility of persons within the European Union has led to a growing number of situations in which family relationships are established in one state while their legal effects are sought in another.⁵ In cross-border family situations, these differences create significant legal challenges, particularly in relation to legal certainty and the continuity of personal status.⁶ Private international law therefore plays a central role in addressing the fragmentation of legal relationships across member states.⁷ In the doctrine of private international law, the recognition of personal statuses has traditionally been regarded as one of the fundamental elements in ensuring legal certainty and the stability of legal relationships.⁸ The non-recognition of a status lawfully acquired abroad may lead to the phenomenon of so-called "limping" legal relationships, in which the same individual holds a different status depending on the state in which they are located.⁹ Furthermore, the fragmentation of personal

¹ Majstorović, I., *Family Law as Diversity in Unity: The European Union and Croatia*, in: Bodiřoga-Vukobrat, N.; Hlaća, N.; Hrabar, D. (eds.), *European Family Law*, Official Gazette, Zagreb 2013., p. 1.

² *European Family Law (PIL)*, Max-EuP 2012, Max Planck Encyclopedia of European Private Law, available at: [https://max-eup2012.mpipriv.de/index.php/European_Family_Law_\(PIL\)](https://max-eup2012.mpipriv.de/index.php/European_Family_Law_(PIL)), accessed 25 January 2026.

³ *Ibid.*

⁴ Garayova, L., *Parenthood without Borders – Judicial Cooperation for Cross-Border Family Security in the EU*, ECLIC, International Scientific Conference: Strong and Secure Europe: Legal and Economic Aspects, Faculty of Law, University of Osijek, 9/2025., p. 326–327.

⁵ European Parliament, *Cross-Border Legal Recognition of Parenthood in the EU*, Policy Department for Citizens' Rights and Constitutional Affairs, PE 746.632, 2023., p. 6–9.

⁶ *Ibid.*

⁷ Sajko, K., *Private International Law*, 5th ed., Official Gazette, Zagreb 2009., p. 7–16.

⁸ See Hlaća, N., *Personal Status of Citizens in the European Union*, in: Bodiřoga-Vukobrat, N. et al., *European Family Law*, Official Gazette, Zagreb 2013., p. 105–143.

⁹ Lagarde, P., *Recognition and Registration of Civil Status Documents in Cross-Border Cases*, Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Brussels 2010., p. 7–8.

status in the area of parent-child relationships carries particular legal significance, as the non-recognition of parental status in cross-border situations creates concrete legal and practical difficulties that may restrict the exercise of freedom of movement within the European Union, while directly affecting the rights of children.¹⁰ Faced with these difficulties, states have traditionally relied on the concept of public policy as a corrective mechanism in the recognition of foreign legal relationships. While public policy serves to protect the fundamental values of the national legal order, its application in cross-border family situations creates a tension between regulatory autonomy and the effective protection of fundamental rights.¹¹ In this context, growing attention has been devoted to the role of fundamental rights in shaping approaches to the recognition of family relationships.¹² The right to private and family life, the right to identity, and the requirements of legal certainty are gradually gaining importance as criteria for assessing the justification of national restrictions in the field of recognition of personal statuses.¹³ Particular emphasis is placed on the position of the child as a holder of independent rights, whose interests do not necessarily coincide with the regulatory interests of the state.¹⁴ In this context, European case law has gradually shifted its analytical focus from the permissibility of specific family law institutions under national law to the legal effects of relationships lawfully established in another member state.¹⁵ This shift allows for a distinction between the non-recognition of a family law institution as such and the obligation to recognise its legal effects where this is necessary for the protection of fundamental rights.¹⁶ In legal doctrine, this approach is described as a functional approach to recognition, which seeks to address the fragmentation of personal status in cross-border situations while preserving the regulatory autonomy of member states.¹⁷ This paper proceeds from a clearly defined research question: can a functional approach to the recognition of family relationships be identified as a common methodological framework in the case law of European courts, and what are its limits in relation to traditional private international law mechanisms, in particular public policy and its attenuated effect (*effet atténué*)?

¹⁰ European Parliament, *op. cit.* in fn. 5, p. 7–8, 15–16.

¹¹ See Sajko, K., *op. cit.* in fn. 7, p. 256–269.

¹² Coman and others, application C-673/16, judgment of 5 June 2018, paras. 37–42.

¹³ Mennesson v France, application no. 65192/11, judgment of 26 June 2014, paras. 37–42.

¹⁴ *Ibid.*

¹⁵ See Scherpe, J. M., *Epilogue to the Family in EU Law – Is there a European Family Law?*, in: Part IV – The EU Family in Internal and External Crises, Cambridge University Press, 2024., p. 249–262.

¹⁶ Coman, *op. cit.* in fn. 12.

¹⁷ See Palazzo, N., *Functional Recognition and Polyamory: Glitters and Hard Truths in the O'Neill Judgment*, Journal of Social Welfare and Family Law, Vol. 46, No. 2/2024., p. 187–207.

In methodological terms, the paper adopts a doctrinal approach based on the analysis of the case law of the European Court of Human Rights (hereinafter ECtHR) and the Court of Justice of the European Union (hereinafter: ECJ). The structure of the paper is as follows. First, the concept of personal status and its relevance in cross-border situations is outlined. This is followed by an analysis of the case law of the ECtHR, and subsequently of the ECJ. Finally, the paper offers a critical assessment of the functional approach and its relationship to traditional private international law mechanisms. Proceeding from the above, the paper advances the thesis that the judgments of the ECJ in *Coman*¹⁸ and *Pancharevo*,¹⁹ as well as more recent case law, although delivered in the context of the free movement of EU citizens, further elaborated a doctrinal framework for a limited and functional approach to the recognition of family relationships created in other member states. Early elements of a functional approach to the recognition of family relationships can be identified in the case law of the ECtHR in particular in the judgments *Mennesson*²⁰ and *Labassee*²¹, which constitute a starting point for examining its further development in the case law of the ECJ. Particular attention is devoted to the position of children, whose rights are especially vulnerable in such situations, given that the consequences of the non-recognition of parental relationships directly affect their legal identity and legal certainty. In such cases, the limits of state autonomy in the field of family law and the obligation to protect the rights of children guaranteed by Article 8 of the European Convention on Human Rights (hereinafter: ECHR)²² are considered simultaneously. In this context, as a starting point for the further analysis, the paper first examines the concept of personal status and its significance in cross-border situations.

2. RECOGNITION OF PERSONAL STATUS IN CROSS-BORDER SITUATIONS

The personal status of a natural person encompasses a set of legally relevant personal characteristics that distinguish that person from others and determine their position within the legal order. These are legal facts connected to the individual from which rights and obligations arise whose effects operate *erga*

¹⁸ *Coman, op. cit.* in fn. 12.

¹⁹ *V.M.A. v Stolichna obshtina, rayon 'Pancharevo'*, Case C-490/20, Judgment of 14 December 2021.

²⁰ *Mennesson, op. cit.* in fn. 13.

²¹ *Labassee v France*, Application No. 65941/11, Judgment of 26 June 2014.

²² European Convention for the Protection of Human Rights and Fundamental Freedoms, Official gazette – International Treaties, No. 18/1997, 6/1999, 14/2002, 13/2003, 9/2005, 1/2006, 2/2010, 13/2017.

omnes, irrespective of a specific legal relationship.²³ Although certain elements of personal status may be subject to change during a person's lifetime, they at any given moment constitute the basis for determining that person's legal position.²⁴ In the classical understanding, elements of personal status include, *inter alia*, name, gender, nationality, domicile, and family status.²⁵ Certain elements of personal status thereby have particular functional importance for the legal order, as they serve as connecting factors for the exercise of various public law and private law effects.²⁶ Within family status, marital status and parenthood are especially prominent, as these relationships produce wide legal effects and play a central role in shaping an individual's legal identity.²⁷ Marriage determines the legal position of an individual in relation to another person, while parenthood establishes the fundamental legal relationship between parent and child, with lasting consequences for both parties.²⁸ Such relationships carry particular normative weight, since their creation, modification, or termination directly affects the legal position of the individual. This is particularly evident in the area of parenthood, which does not only shape the legal status of adults but also produces long-term legal effects in relation to children, especially with regard to their identity, legal belonging to a family, and legal certainty.²⁹ Precisely because of these effects, legal doctrine emphasises that matters of personal status, although formally belonging to the sphere of private law, simultaneously possess a pronounced dimension of fundamental rights protection.

In cross-border situations, the legal significance of personal status becomes particularly evident. The freedom of movement of persons within the European Union leads to increasingly frequent situations in which elements of personal status, such as marital status or parenthood, are acquired or established in one state while their legal effects are sought in another.³⁰ In such circumstances, the non-recognition of a personal status lawfully acquired abroad may lead to situations in which the same person does not enjoy an equal legal position in different legal orders. Such inconsistency is particularly visible in the field of family

²³ Trabucchi, A., *Istituzioni di diritto civile*, 27th ed., Cedam, Padova 1985., p. 4.

²⁴ Hlača, N., *op. cit.* in fn. 8, p. 107.

²⁵ *Ibid.*

²⁶ *Ibid.*, p. 108.

²⁷ *Loc. cit.*

²⁸ *Ibid.*, p. 106–107.

²⁹ Mennesson, *op. cit.* in fn. 13 and Labassee, *op. cit.* in fn. 21.

³⁰ Hlača, N., *op. cit.* in fn. 8, p. 111.

relationships, as it may have serious consequences for legal certainty and the continuity of family life.³¹

The recognition of elements of personal status in cross-border situations is generally achieved through the recognition of foreign public documents, thereby enabling a status lawfully established in one state to produce effects in another.³² In this context, legalisation, including the institution of the *apostille*³³, has long represented a fundamental mechanism for confirming the authenticity of foreign documents in legal transactions. Although the *apostille*³⁴ remains relevant in relations with third countries, its application within the European Union has been significantly limited. Regulation (EU) 2016/1191 abolished the requirement of legalisation and *apostille* for certain public documents relating to personal status, with the aim of reducing administrative obstacles and facilitating the free movement of persons. However, this Regulation does not govern the recognition of the substantive legal effects of personal status, which remains within the competence of national legal orders. This clearly distinguishes the formal recognition of documents from the recognition of personal status itself, a distinction that carries particular normative importance in the context of cross-border family relationships.³⁵ The limitations of such a formal approach to the recognition of personal status are especially evident in situations where the non-recognition of the legal effects of a status may result in a violation of fundamental rights, particularly the right to private and family life and the right to identity. In such circumstances, an approach is gradually emerging that does not place exclusive emphasis on the formal recognition of documents but rather on the recognition of the concrete legal effects of personal status to the extent necessary to ensure legal certainty and effective legal protection. This establishes a normative framework for the analysis of the functional approach to the recognition of family relationships in cross-border situations, which will be examined in the following sections through the case law of the ECtHR and subsequently through the case law of the ECJ.

³¹ Corneloup, S.; Heiderhoff, B.; Honorati, C. (eds.), *Private International Law in a Context of Increasing International Mobility: Challenges and Potential*, Study for the JURI Committee, European Parliament, 2017., p. 9–11.

³² Regulation (EU) 2016/1191 of the European Parliament and of the Council of 6 July 2016 on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents in the European Union and amending Regulation (EU) No. 1024/2012, OJ L 200, 26 July 2016. (hereinafter: Regulation (EU) 2016/1191.

³³ The apostille institute is regulated by the Hague Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents, Official Gazette – International Treaties, No. 4/4, 11/11; Official Gazette of the FPRY – International Treaties, No. 10/62.

³⁴ Regulation (EU) 2016/1191, *op. cit.* in fn. 32.

³⁵ *Ibid.*

3. CASE LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS

Proceeding from the previously outlined normative framework for the recognition of personal status in cross-border situations, it is first necessary to examine the case law of the ECtHR in cases concerning surrogacy and the recognition of family relationships established abroad. Although the ECtHR operates within a different normative framework and proceeds from the protection of rights guaranteed by the ECHR,³⁶ its case law has played an important role in shaping standards for the protection of personal status and family life in cross-border situations. Particular importance in this regard attaches to the judgments in *Mennesson*³⁷ and *Labassee*³⁸, in which the ECtHR for the first time examined the effects of the non-recognition of parenthood established through surrogacy on the rights of children born abroad.

In those cases, the ECtHR devoted particular attention to the protection of the rights of children, especially the right to identity and the right to private and family life guaranteed by Article 8 of the ECHR, thereby limiting the ability of states to call into question the continuity of a child's personal status through the non-recognition of a parent-child relationship.³⁹ Such an approach represents an important starting point for understanding the development of a functional approach to the recognition of family relationships in European case law. The analysis of these judgments makes it possible to examine the extent to which early elements of a functional approach to the recognition of family relationships can be identified in the case law of the ECtHR, which will in the following sections be compared with the approach developed in the case law of the ECJ.

3.1. *Mennesson v. France* and *Labassee v. France*

The absence of a European consensus on the permissibility of surrogacy represents a significant challenge for the case law of the ECtHR, particularly in the application of Article 8 of the ECHR. The diversity of national solutions gives rise to complex questions regarding the scope of the right to private and family life and

³⁶ ECHR, *op. cit.* in fn. 22.

³⁷ *Mennesson*, *op. cit.* in fn. 13.

³⁸ *Labassee*, *op. cit.* in fn. 21.

³⁹ *Ibid.*

its potential conflict with the protection of public policy.⁴⁰ The ECtHR therefore regards the achievement of a balance between the general public interest and the interests of the individual as an imperative when examining such cases, particularly in situations where the non-recognition of a parent-child relationship affects the legal status of children born abroad.⁴¹

The judgments in *Mennesson v. France* and *Labassee v. France* represent a turning point in the case law of the ECtHR, as they shift the focus from the permissibility of surrogacy to the legal effects of parenthood established abroad.⁴² In these cases, the ECtHR examined the rights arising from parenthood lawfully established through surrogacy in the United States of America, which were in conflict with French public policy.⁴³ Although the factual circumstances of the two judgments are not identical, given that they raise the same legal issues and that the ECtHR delivered two corresponding judgments on 26 June 2014., the cases will be analysed jointly in the following sections.

3.2. Analysis of *Mennesson* and *Labassee*

Against this background, the ECtHR in *Mennesson v. France* and *Labassee v. France* examined situations in which children were born through surrogacy arrangements lawfully carried out in the United States, with the parent-child relationship formally recognised under US law. Upon returning to France, the applicants sought recognition of that relationship, which was refused by the national authorities on the grounds of public policy and the prohibition of surrogacy.⁴⁴

Although the factual circumstances in *Mennesson v. France* and *Labassee v. France* differ in certain respects, the ECtHR delivered substantively identical judgments in both cases on 26 June 2014. At the core of both cases was the question of whether the national refusal to recognise parenthood lawfully established abroad through surrogacy was compatible with the right to respect for

⁴⁰ Shuilleabhain, M. N., *Surrogacy, System Shopping, and Article 8 of the European Convention on Human Rights*, International Journal of Law, Policy and the Family, Vol. 33, No. 1/2019., p. 115.

⁴¹ Bouček, V., *European Private International Law in the European Integration Process and Selected Issues of the Applicable Law*, Official Gazette, Zagreb 2021., p. 114.

⁴² Fenton-Glynn, C., *International surrogacy before the European Court of Human Rights*, Journal of Private International Law, Vol. 13, No. 3/2017., p. 555.

⁴³ *Mennesson*, *op. cit.* in fn. 13 and *Labassee*, *op. cit.* in fn. 21.

⁴⁴ *Mennesson*, *op. cit.* in fn. 13, paras. 6–28 and *Labassee*, *op. cit.* in fn. 21, paras. 6–17.

private and family life guaranteed by Article 8 of the ECHR.⁴⁵ These cases provided the first systematic opportunity for the ECtHR to examine the limits of state autonomy in protecting public policy in relation to the rights of children in cross-border situations. The ECtHR first established that the refusal to register the parent-child relationship constituted an interference with the rights guaranteed by Article 8 of the ECHR. While this interference was prescribed by law and pursued legitimate aims, including the protection of public policy, the key issue was whether it was proportionate. France relied on the nullity of surrogacy agreements under national law and on the need to discourage recourse to such practices abroad.⁴⁶ The ECtHR further observed that no European consensus exists in the field of surrogacy, which grants States a wide margin of appreciation.⁴⁷ However, it emphasised that this margin is not unlimited and must be assessed in light of the nature and seriousness of the interference with individual rights. It particularly stressed that, where fundamental aspects of children's identity are concerned, the state's margin of appreciation must be narrower.⁴⁸ In this respect, the ECtHR's reasoning is particularly important, as it makes clear that national public policy cannot be applied without limits where fundamental rights are concerned. In that context, the ECtHR clearly distinguished between different aspects of the rights protected under Article 8 of the ECHR. With regard to the intended parents' right to respect for family life, the ECtHR accepted the conclusion of the national courts that the non-recognition of parenthood had not prevented the family from living together in France nor had it led to a de facto severance of family ties. Accordingly, it did not find a violation of Article 8 of the ECHR in that aspect.⁴⁹ By contrast, the ECtHR devoted particular attention to the children's right to respect for private life, which in its view encompasses the right to personal identity and legal certainty. This distinction is central to the ECtHR's reasoning, as it redirects the focus from the interests of the adults to the autonomous rights of the child. By refusing to recognise parenthood lawfully established abroad, the children were placed in a situation of legal uncertainty regarding their origin, nationality, and inheritance rights. Although Article 8 of the ECHR does not guarantee a right to acquire a particular nationality, the ECtHR emphasised that nationality, as well as the legal relationship with one's parents, constitute essential components of a child's identity. Uncertainty concerning these elements may have long-term

⁴⁵ Mennesson, *op. cit.* in fn. 13, para. 43 and Labassee, *op. cit.* in fn. 21, para. 34.

⁴⁶ Mennesson, *op. cit.* in fn. 13, paras. 48–50 and Labassee, *op. cit.* in fn. 21, paras. 33–38.

⁴⁷ Mennesson, *op. cit.* in fn. 13, paras. 76–78 and Labassee, *op. cit.* in fn. 21, paras. 57–58.

⁴⁸ Mennesson, *op. cit.* in fn. 13, paras. 96–100 and Labassee, *op. cit.* in fn. 21, paras. 59–60.

⁴⁹ Mennesson, *op. cit.* in fn. 13, paras. 92–94 and Labassee, *op. cit.* in fn. 21, paras. 71–73, 81.

negative consequences for the child's development and social integration.⁵⁰ Furthermore, the ECtHR considered that a situation in which a state simultaneously acknowledges the existence of family life in a factual sense but refuses to recognise its legal effects leads to an internal contradiction within the legal system. According to the ECHR, such contradictions undermine the children's identity within society and exceed the limits of the state's permissible margin of appreciation, particularly in situations where at least one of the intended parents is also the child's biological parent.⁵¹ This line of reasoning further reinforces the idea that the legal effects of a family relationship cannot be disregarded where doing so would undermine fundamental aspects of a child's identity. It reflects a broader shift in the ECtHR's approach, which prioritises the protection of fundamental rights over the formal acceptance of a particular family law institution. Accordingly, the ECtHR concluded that, although there had been no violation of Article 8 of the ECHR with regard to the intended parents' right to respect for family life, there had been a violation in respect of the children's right to respect for their private life.⁵² The ECtHR thus confirmed that, although states retain broad autonomy to prohibit surrogacy as a family law institution, they are not entitled to completely refuse recognition of the legal effects of parenthood lawfully established abroad where this would undermine the child's fundamental rights.⁵³ This child-centred approach represents an important step towards the development of a functional approach to recognition, as it prioritises the protection of fundamental rights over the formal acceptance of a particular family law institution. It also provides an important starting point for understanding the further development of this approach in the case law of the ECJ, particularly in cases concerning the free movement of European Union citizens.

4. CASE LAW OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

Building on the standards of protection developed in the case law of the ECtHR, this section examines the case law of the ECJ in relation to the recognition of family relationships in cross-border situations. The case law of the ECJ plays a key role in determining the legal effects of non-recognition in the context of free movement and the protection of fundamental rights. In this respect, the ECJ's approach does not question national definitions of family law institutions as such,

⁵⁰ Mennesson, *op. cit.* in fn. 13, paras. 96–101 and Labassee, *op. cit.* in fn. 21, paras. 75–80.

⁵¹ *Ibid.*

⁵² Mennesson, *op. cit.* in fn. 13, para. 102 and Labassee, *op. cit.* in fn. 21, para. 81.

⁵³ *Ibid.*

but rather focuses on their legal effects where necessary to ensure the effectiveness of EU law.

Against this background, the judgments in *Coman*⁵⁴ and *Pancharevo*⁵⁵, as well as more recent case law, are examined as key examples of the further development of a functional approach to the recognition of family relationships in EU law. In those cases, the ECJ examined the extent to which member states, while retaining autonomy in the field of family law, are nevertheless required to recognise certain legal effects of family relationships lawfully established in other member states. These cases demonstrate a shift from the question of whether a family relationship must be recognised as such to the question of which legal effects must be recognised in order to safeguard rights derived from EU law.

4.1. *Coman*

The judgment of the ECJ in *Coman* represents a significant development in the case law concerning the recognition of the legal effects of family relationships in cross-border situations within the European Union. Although delivered in the context of the free movement of Union citizens, the judgment has broader implications, particularly regarding the limits within which member states may refuse to recognise a family relationship without infringing rights derived from EU law.⁵⁶ In *Coman*, the ECJ did not address the recognition of same-sex marriage as a family law institution as such, but rather focused on the legal effects arising from such a relationship in a cross-border context.⁵⁷ This distinction is central to the ECJ's reasoning, as it reflects a functional approach to recognition based on the effects of a relationship rather than its formal acceptance under national law. In doing so, the ECJ addressed the relationship between member states' autonomy in regulating family law and the requirements of free movement under EU law.⁵⁸ The case thus forms part of a broader line of case law in which the ECJ assesses the impact of national rules on personal status on the effective exercise of rights guaranteed under EU law.

The case concerned a Romanian national who, during residence in another member state, entered into a same-sex marriage with a third-country national.

⁵⁴ *Coman*, *op. cit.* in fn. 12.

⁵⁵ *Pancharevo*, *op. cit.* in fn. 19.

⁵⁶ Frattone, C., *Same-sex spouses' rights in the ECJ's Coman case*, *Roma Tre Law Review*, No. 2/2019., p. 303–305.

⁵⁷ *Ibid.*

⁵⁸ *Coman*, *op. cit.* in fn. 12, paras. 37–38.

Upon returning to Romania, the spouse applied for a right of residence exceeding three months as a family member of a Union citizen. The Romanian authorities refused the request, relying on national provisions prohibiting same-sex marriage and its recognition, including marriages concluded abroad. This refusal resulted in the denial of legal effects of a marriage lawfully concluded in another member state, solely due to differences in national family law.⁵⁹ The dispute therefore raised the issue of the fragmentation of personal status within the Union and the possibility that a Union citizen, upon returning to their own member state, might lose the legal continuity of the family life established in another member state. The case thus illustrates the problem of fragmentation of personal status within the Union and raises the question of whether such fragmentation is compatible with the effective exercise of free movement rights.

From a legal perspective, the case was situated at the intersection of primary and secondary EU law. On the one hand, Article 21(1) of the Treaty on the Functioning of the European Union (hereinafter: TFEU)⁶⁰ guarantees Union citizens the right to move and reside freely within the territory of the member states.⁶¹ In addition, Directive 2004/38/EC (hereinafter: the Directive)⁶² governs the right of residence of family members, including the definition of "family member". Although the Directive formally applies to situations where a Union citizen resides in a member state other than that of their nationality, the ECJ, following its settled case law, applied it by analogy to situations involving the return of a Union citizen to their member state of origin.⁶³ In doing so, the ECJ emphasised the need to ensure the effectiveness of the freedom of movement. If a Union citizen, upon returning to their own member state, were prevented from living with a family member with whom they had established a family life in another member state, the freedom of movement would be seriously restricted. Such an outcome could have a deterrent effect on the exercise of the right to free movement, which is incompatible with the fundamental objectives of Union law.⁶⁴ In this context, the ECJ focused not on the formal recognition of the marriage under national law, but on the necessity of

⁵⁹ *Ibid.*, paras. 45–49.

⁶⁰ Consolidated version of the Treaty on the Functioning of the European Union, OJ C 202/49, 7 June 2016.

⁶¹ Coman, *op. cit.* in fn. 12, para. 18.

⁶² Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States, amending Regulation (EEC) No. 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC, OJ L 158, 30 April 2004.

⁶³ Coman, *op. cit.* in fn. 12, paras. 20–24.

⁶⁴ Gyeney, L., *Same Sex Couples' Right to Free Movement in Light of Member States' National Identities: The Legal Analysis of the Coman Case*, *Iustum Aequum Salutare*, Vol. 14, No. 2/2018., p. 162–163.

recognising its legal effects in order to ensure the effective exercise of free movement rights.

4.1.1. Analysis of Coman

In *Coman*, the ECJ examined the relationship between member states' competence in the field of personal status and the obligations arising under EU law in cross-border situations involving the exercise of free movement. The dispute concerned the legal effects of the national non-recognition of a same-sex marriage lawfully concluded in another member state, in the context of a Union citizen returning to the member state of their nationality. The case therefore raised the question of whether national rules on personal status may limit the exercise of rights derived from EU law in cross-border situations.⁶⁵ The ECJ recalled that Union citizenship, under Article 20 TFEU, is intended to be the fundamental status of nationals of the member states and entails the right to move and reside freely, including the possibility of leading a normal family life.⁶⁶ A Union citizen who has exercised free movement may therefore rely on rights under Article 21(1) TFEU also vis-à-vis their member state of nationality.⁶⁷ This confirms that the rights derived from Union citizenship extend beyond purely internal situations where a cross-border element is present. The non-recognition of a family relationship established during residence in another member state therefore cannot be regarded as an exclusively internal matter of national family law, but rather as an issue falling within the scope of Union law due to its effects in a cross-border situation.⁶⁸ The central element of the ECJ's reasoning concerned the interpretation of the term "spouse" within the meaning of Directive 2004/38, applied by analogy in situations involving the return of a Union citizen. The ECJ recalled that Article 2(2)(a) of the Directive expressly lists the "spouse" as a family member. On that basis, the ECJ concluded that the term "spouse" constitutes an autonomous concept of Union law and is gender-neutral. This interpretation is central to the ECJ's approach, as it treats the concept of "spouse" as an autonomous notion of EU law, independent of national definitions. Consequently, it may include the same-sex spouse of a Union citizen, provided that the marriage was lawfully concluded in another member state in

⁶⁵ Kochenov, D.; Belavusau, U., *Same-sex spouses in the EU after Coman: More free movement, but what about marriage?*, EUI Working Paper LAW, No. 3/2019., p. 1–2 and 5–6.

⁶⁶ *Coman*, *op. cit.* in fn. 12, paras. 29–32.

⁶⁷ *Ibid.*, paras. 31–32.

⁶⁸ Tryfonidou, A., *The ECJ Recognises the Right of Same-Sex Spouses to Move Freely between EU Member States: The Coman Ruling*, *European Law Review*, Vol. 44, No. 5/2019., p. 16–18.

accordance with the law of that state.⁶⁹ In this way, the ECJ ensures that the legal effects of marriage are recognised for the purposes of EU law without requiring member states to recognise the institution of same-sex marriage as such. A member state may not rely on its own national law in order, solely for the purpose of granting a derived right of residence, to refuse recognition of such a marriage.⁷⁰ This confirms that national rules on personal status cannot be relied upon where they undermine the effectiveness of rights derived from EU law. At the same time, the ECJ expressly confirmed that personal status, including rules on marriage, in principle falls within the competence of the member states and that Union law does not impose an obligation to introduce or generally recognise same-sex marriage.⁷¹ However, that competence must be exercised in compliance with Union law, in particular the right of Union citizens to move and reside freely guaranteed by Article 21(1) TFEU. National rules on personal status cannot produce effects that lead to a restriction of the rights conferred on Union citizens under the Treaty.⁷² This reflects a balance between member states' regulatory autonomy and the requirements of EU law, whereby national competence is preserved, but its effects are limited where they interfere with the exercise of free movement rights. The ECJ further observed that allowing member states, depending on national law, to grant or refuse residence to the same-sex spouse of a Union citizen would result in the uneven application of the freedom of movement within the Union. Such an approach would be contrary to the objectives of Directive 2004/38, as the exercise of the freedom of movement would become dependent on the legislation of a particular member state.⁷³ Moreover, refusal to recognise the marriage for the purpose of residence could prevent a Union citizen from returning to the member state of their nationality accompanied by their spouse, thereby seriously restricting the exercise of the rights under Article 21(1) TFEU.⁷⁴ This highlights that national divergences in the regulation of personal status cannot lead to obstacles to the uniform application of free movement rights within the Union. In examining the justification for such a restriction, the ECJ addressed arguments based on public policy and national identity.⁷⁵ It emphasised that the concept of public policy must be interpreted restrictively and may be relied upon only where there is a genuine and sufficiently serious threat to a fundamental interest of society.⁷⁶ The obligation to recognise a same-sex marriage solely for the purpose of granting a right of residence to the spouse does not affect the

⁶⁹ *Ibid.*, para. 35.

⁷⁰ *Ibid.*, para. 36.

⁷¹ *Ibid.*, para. 37.

⁷² *Ibid.*

⁷³ Tryfonidou, A., *op. cit.* in fn. 68, p. 6–7.

⁷⁴ Coman, *op. cit.* in fn. 12, para. 40.

⁷⁵ *Ibid.*, para. 42.

⁷⁶ *Ibid.*

institution of marriage in the national law of the member state nor does it require any amendment to its family legislation. Such an obligation therefore does not interfere with the national identity of the member state nor does it constitute a threat to public policy.⁷⁷ This demonstrates that public policy cannot be invoked where it would undermine the effectiveness of rights derived from EU law. The ECJ further emphasised that any restriction on the freedom of movement must also be assessed in the light of the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union.⁷⁸ In that regard, the ECJ highlighted the right to respect for private and family life under Article 7 of the Charter, which has the same meaning and scope as Article 8 of the ECHR.⁷⁹ Referring to the case law of the ECtHR, the ECJ confirmed that the relationship of a same-sex couple may constitute family life and private life to the same extent as the relationship of a heterosexual couple in a comparable situation.⁸⁰

Accordingly, in its response to the questions referred for a preliminary ruling, the ECJ held that Article 21(1) TFEU precludes a member state from refusing, in a situation where a Union citizen has genuinely and lawfully exercised the freedom of movement and has created or strengthened a family life in another member state with a same-sex spouse, to grant that spouse a right of residence solely on the ground that national law does not provide for same-sex marriage. The ECJ further clarified that the same-sex spouse, as a third-country national, has the right to reside for more than three months in the member state of which the Union citizen is a national, and that this right must not be made subject to conditions more stringent than those laid down in Article 7 of Directive 2004/38.⁸¹ According to *Rijpma*, it follows from the content of the *Coman* judgment that ECJ does not introduce an obligation of general recognition of same-sex marriage as a family law institution, but rather establishes a model of a limited, functional approach to recognition. member states are required to recognise the legal effects of personal status lawfully acquired in another member state to the extent necessary for the exercise of the rights conferred on Union citizens under Union law. Such an approach allows for the preservation of the regulatory autonomy of member states in the field of family law while simultaneously preventing the fragmentation of personal status and ensuring the continuity of family life in cross-border

⁷⁷ Tryfonidou, A., *op. cit.* in fn. 68, p. 11–12 and *Coman*, *op. cit.* in fn. 12, paras. 45–46.

⁷⁸ Charter of Fundamental Rights of the European Union, OJ C 202/389, 7. 6. 2016. (hereinafter Charter)

⁷⁹ *Coman*, *op. cit.* in fn. 12, paras. 47–48.

⁸⁰ *Ibid.*, para. 50.

⁸¹ *Ibid.*, para. 58.

situations.⁸² This further confirms the development of an approach which, similarly to the case law of the ECtHR, distinguishes between the non-recognition of a family law institution and the obligation to recognise its legal effects where this is necessary for the protection of fundamental rights.

The Coman judgment therefore goes beyond the specific issue of residence rights and establishes a broader doctrinal framework for limiting national autonomy in the field of personal status where this affects rights guaranteed under EU law. The functional approach to recognition, grounded in the protection of fundamental rights and the effectiveness of free movement, can be regarded as one of the central methodological elements in the case law of the ECJ. This approach is further developed in the Pancharevo judgment, particularly in the context of parent-child relationships and the legal identity of the child, with a strong emphasis on the best interests of the child and the continuity of personal status within the European Union.

4.2. Pancharevo

The Pancharevo case opens a discussion on one of the central issues of European Union law in the field of cross-border family relationships, namely ensuring the effective protection of children in situations in which their personal status and the parent-child relationship do not correspond to the legal solutions of the member states in which they reside.⁸³ The case concerns a situation in which a child born in one member state was issued a birth certificate indicating two mothers, while another member state refused to recognise that parent-child relationship for the purposes of issuing an identity document. This refusal raised the question of whether such non-recognition could restrict the child's right to free movement and undermine the continuity of their personal status within the European Union.⁸⁴ In this context, the question of recognising a parental relationship cannot be assessed solely from the perspective of national autonomy in family law, but must be examined in light of the effects that such non-recognition produces on the child's fundamental rights. The central legal problem in Pancharevo therefore concerns the limits within which member states may refuse recognition of a parental relationship without undermining the child's status as a holder of rights under EU

⁸² Rijpma, J. J., *You Gotta Let Love Move: ECJ 5 June 2018, Case C-673/16, Coman, Hamilton, Accept v Inspectoratul General pentru Imigrări*, European Constitutional Law Review, Vol. 15, No. 2/2019., p. 327–335.

⁸³ Pancharevo, *op. cit.* in fn. 19.

⁸⁴ See Pancharevo, *op. cit.* in fn. 19, paras. 18–32.

law.⁸⁵ This suggests the need to examine a legal framework that balances member states' regulatory autonomy with the recognition of certain legal effects of the parent-child relationship where necessary to protect the child's identity, legal certainty, and freedom of movement.

4.2.1. Analysis of Pancharevo

The case concerned a Bulgarian national who, together with her spouse, resided in another member state, where their child was born and was issued a birth certificate listing both women as parents. The Bulgarian authorities refused to register the child in the national civil registry and to issue an identity document, relying on national law, which does not recognise same-sex parenthood and considers such recognition contrary to public policy.⁸⁶ As a result, the child, despite holding the nationality of a member state, was placed in a situation in which the effective exercise of the right to free movement was jeopardised.⁸⁷ The referring court therefore raised the question of whether such non-recognition was compatible with Articles 20 and 21 TFEU,⁸⁸ read in conjunction with the Charter of Fundamental Rights of the European Union⁸⁹, in particular the rights to private and family life and the best interests of the child.⁹⁰

The request for a preliminary ruling also addressed the relationship between national identity and EU law, as well as the extent to which member states may rely on public policy in order to refuse recognition of a parent-child relationship established in another member state.⁹¹ In essence, the case required the ECJ to determine the relationship between national competence in the field of family law and the obligations arising under EU law in cross-border situations.⁹² Against this background, the ECJ proceeded to examine the case within the framework of EU

⁸⁵ Marinkás, G., *Some Remarks on the CJEU's 'Pancharevo' Decision with Special Regard to the Nexus between the Primacy of EU Law and the National Identity of Member States*, Law, Identity and Values, Vol. 3, No. 1/2023., p. 190.

⁸⁶ De Groot, D. A. J. G., *Special Report: EU Law and the Mutual Recognition of Parenthood between Member States: The Case of V.M.A. v Stolichna obshtina*, RSCAS/GLOBALCIT Special Report, Robert Schuman Centre for Advanced Studies, European University Institute, No. 1/2021., p. 1–2.

⁸⁷ Pancharevo, *op. cit.* in fn. 19, para. 26.

⁸⁸ TFEU, *op. cit.* in fn. 60.

⁸⁹ Charter of Fundamental Rights of the European Union, *op. cit.* in fn. 78.

⁹⁰ Pancharevo, *op. cit.* in fn. 19, paras. 28–30.

⁹¹ *Ibid.*, para. 32, points 1–4.

⁹² Luku, H., *The Supreme Administrative Court of Bulgaria's Final Decision in the Pancharevo Case: Bulgaria Is Not Obligated to Issue Identity Documents for Baby S.D.K.A. as She Is Not Bulgarian (but Presumably Spanish)*, Conflict of Laws, 2023., p. 1–5.

law. The case was approached not as a question of recognising a family law institution as such, but as a question concerning the effects of non-recognition on the exercise of rights derived from EU law.⁹³ The ECJ begins its analysis with the fact that the child acquired the nationality of a member state and that, pursuant to Article 20 TFEU, the child holds the status of a Union citizen.⁹⁴ Relying on settled case law according to which Union citizenship is intended to be the fundamental status of nationals of the member states, the ECJ places the case within the scope of Union law.⁹⁵ This excludes the possibility of treating the matter as an exclusively internal issue of national family law, regardless of the national legal qualification of the parental relationship. On that basis, the ECJ further develops its approach to the interpretation of Article 21 TFEU. Freedom of movement and residence is not interpreted as an abstract right, but as a right that must be genuinely and effectively exercisable. This means that member states cannot rely on formal or procedural requirements where their application would render the exercise of free movement rights ineffective. In this context, the ECJ links the obligation to issue identification documents with the effective application of Union law and expressly rejects the possibility for a member state to rely on its own procedural or formal requirements where their application creates obstacles to the exercise of the rights of a Union citizen.⁹⁶ This confirms that national rules on personal status cannot have autonomous effect insofar as they lead to the derogation of the effects of Union law. The central element of the ECJ's reasoning concerns the recognition of the parent-child relationship established in another member state. The ECJ proceeds from the fact that the parental relationship between the child and the two mothers was lawfully established in the member state of the child's birth and confirmed by a public document issued in accordance with the law of that state.⁹⁷ Accordingly, the Bulgarian authorities, like the authorities of any other member state, are required to recognise that parental relationship in order to enable the child to exercise, with each of her two parents, the right to move and reside freely within the territory of the member states, as guaranteed by Article 21(1) TFEU.⁹⁸ Instead of examining the substantive compatibility of that relationship with the national family law of the member state of which the child is a national, the ECJ analyses the consequences of non-

⁹³ *Functional Recognition of Same-sex Parenthood for the Benefit of Mobile Union Citizens – Brief Comments on the CJEU's Pancharevo Judgment*, available at: <https://eapil.org/2022/02/03/functional-recognition-of-same-sex-parenthood-for-the-benefit-of-mobile-union-citizens-brief-comments-on-the-cjeus-pancharevo-judgment/>, accessed 30 January 2026.

⁹⁴ Pancharevo, *op. cit.* in fn. 19, para. 40.

⁹⁵ *Ibid.*, para. 41.

⁹⁶ *Ibid.*, paras. 41–46.

⁹⁷ *Ibid.*, para. 48.

⁹⁸ *Ibid.*, para. 49.

recognition in a cross-border context. This confirms that the ECJ does not assess the validity of the parental relationship under national law, but rather its legal effects in a cross-border context. The non-recognition of the parental relationship is assessed solely in light of its effect on the child's ability to exercise, together with each of her parents, the right to free movement and residence.⁹⁹ In doing so, the ECJ expressly establishes a model of a limited, functional approach to the recognition of family relationships. A member state is therefore required to recognise the parental relationship only to the extent necessary for the exercise of the rights that the child derives from Union law. This reflects a functional approach to recognition, whereby the obligation of recognition is limited to what is necessary to ensure the effective exercise of rights derived from EU law. Such an obligation does not entail recognition of same-sex parenthood as an institution of national family law, nor does it produce effects outside the scope of Union law. In this way, the ECJ deliberately avoids normative unification of family law while simultaneously preventing the fragmentation of the child's personal status within the legal space of the Union.¹⁰⁰ With regard to reliance on national identity and public policy, the ECJ adopts a restrictive approach and limits the scope of those concepts in the context of EU law. Article 4(2) Treaty on European Union¹⁰¹ cannot be interpreted as an autonomous basis for derogation from Union law, but rather as a provision whose application remains subject to the requirements of the union's fundamental freedoms and fundamental rights.¹⁰² This confirms that national identity and public policy cannot be invoked as autonomous grounds for refusing recognition where such refusal would undermine the effectiveness of rights derived from EU law. The ECJ expressly emphasises that the obligation arising from the functional approach to recognising the parental relationship does not interfere with the fundamental political and constitutional structures of a member state, as it does not require any amendment of national family legislation nor the general acceptance of such a parental relationship in national law.¹⁰³ The ECJ places particular emphasis on the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private and family life and the rights of the child.¹⁰⁴ The right to free movement is interpreted in inseparable connection with the obligation to safeguard the best interests of the child, while the non-recognition of the parental relationship is assessed as a measure capable of leading to legal uncertainty, undermining

⁹⁹ *Ibid.*

¹⁰⁰ *Ibid.*, para. 52.

¹⁰¹ Treaty on European Union, OJ C 202, 7.6.2016. (hereinafter TEU)

¹⁰² Pancharevo, *op. cit.* in fn. 19, paras. 54–55.

¹⁰³ *Ibid.*, para. 57.

¹⁰⁴ *Ibid.*, paras. 59–65.

identity, and effectively preventing the exercise of the rights of a Union citizen.¹⁰⁵ This confirms that the child's rights are not treated as ancillary, but as a central element in determining the scope of member states' obligations under EU law. By referring to the case law of the ECtHR, the ECJ confirms that the existence of family life depends on the reality of family relationships rather than on the formal structure of the family.¹⁰⁶ In its response to the questions referred, the ECJ therefore concludes that Union law requires the member state of which the child is a national to issue the child with an identification document for the purpose of exercising the right to free movement, irrespective of the issuance of a national birth certificate, and, in that context, to recognise the parental relationship lawfully established in another member state. Such recognition is limited to the purpose of exercising the rights that the child derives from Union law and does not produce effects within national family law beyond that framework.¹⁰⁷

The Pancharevo judgment confirms the doctrinal consistency of the ECJ's case law, particularly in relation to Coman. The Court does not call into question the competence of member states in the field of family law, nor does it impose an obligation of general recognition of family relationships not provided for under national law. However, it clearly delineates the limits of national regulatory autonomy where its exercise leads to a restriction of rights derived from EU law.

Through this approach, the ECJ confirms the doctrine of the functional approach to the recognition of family relationships as an instrument for ensuring the effectiveness of the rights of Union citizens in cross-border situations. In this respect, the obligation of recognition is limited to the legal effects necessary to ensure the effective exercise of rights derived from EU law. This approach also indicates a significant degree of convergence with the standards developed in the case law of the ECtHR, particularly with regard to the protection of children's identity and legal certainty in cross-border situations. The normative significance of the Pancharevo judgment thus extends beyond the field of free movement in the narrow sense and points to broader implications for European standards of child protection and legal certainty in transnational family relationships. In this respect, the Pancharevo judgment represents one of the clearest expressions of the functional approach to the recognition of family relationships in the case law of the ECJ.

¹⁰⁵ *Ibid.*, paras. 46, 49, 65.

¹⁰⁶ *Ibid.*, paras. 60–62.

¹⁰⁷ *Ibid.*, para. 70.

4.3. Further development of the functional approach in recent ECJ case law

The approach developed in the case law of the ECJ, particularly in *Coman* and *Pancharevo*, has been further elaborated in more recent judgments, notably *Mirin*¹⁰⁸ and *Cupriak-Trojan*.¹⁰⁹ These cases provide additional insight into the scope and limits of the functional approach to the recognition of personal status in cross-border situations, while also revealing a certain differentiation in its application depending on the nature of the personal status concerned.

In *Mirin*, the ECJ addressed a situation concerning the recognition of a change of name and gender identity lawfully established in another member state. The applicant, a Union citizen, had obtained legal recognition of his gender transition abroad and subsequently sought the registration of that change in the member state of origin. The national authorities refused, requiring the initiation of a new domestic procedure. The ECJ held that such a requirement constitutes a restriction on the exercise of the right to free movement, as it places the individual in a situation of legal uncertainty and may lead to inconsistencies in identity documents. In its reasoning, the ECJ went beyond a strictly functional understanding of recognition. It required not only the recognition of certain legal effects, but also the recognition and registration of the change in order to ensure the continuity of the individual's legal identity across member states. The obligation imposed on the member state of origin thus extended to the registration of the change in official records, ensuring the continuity of the individual's legal identity across legal systems. This approach reflects a stronger emphasis on the protection of personal identity as a fundamental right, closely linked to human dignity and legal certainty.¹¹⁰

By contrast, in *Cupriak-Trojan*, the ECJ reaffirmed the functional approach developed in *Coman* and *Pancharevo* in the context of same-sex marriage. The case concerned the refusal of a member state to recognise and register a same-sex marriage lawfully concluded in another member state. The ECJ held that such a refusal may constitute a restriction on the exercise of the right to free movement, particularly where it prevents individuals from leading a normal family life in the member state of origin. However, the ECJ maintained the distinction between the recognition of a family law institution as such and the recognition of its legal effects. It confirmed that member states are not required to introduce or generally

¹⁰⁸ *Mirin*, Case C-4/23, Judgment of 4 October 2024.

¹⁰⁹ *Cupriak-Trojan*, Case C-713/23, Judgment of 5 December 2024.

¹¹⁰ Tryfonidou, A., *The Cross-Border Recognition of Changes in the Legal Sex of Transgender Persons: The Landmark Court of Justice Ruling in the Mirin Case*, *European Constitutional Law Review*, Cambridge University Press, 2025., p. 333–355.

recognise same-sex marriage in their national legal orders. At the same time, they are required to recognise and give effect to such a marriage to the extent necessary to ensure the effective exercise of rights derived from EU law. The obligation of recognition thus remains limited in scope and functionally determined.¹¹¹

When considered together, these judgments demonstrate that the functional approach to recognition, although consistently applied as a methodological framework, is not uniform in its intensity. In cases such as *Cupriak-Trojan*, the ECJ adheres to a limited model of recognition focused on specific legal effects necessary for the exercise of free movement rights. In contrast, in *Mirin*, the ECJ requires a more extensive form of recognition where this is necessary to safeguard fundamental aspects of personal identity and to avoid situations of legal fragmentation. This development suggests that the functional approach is evolving into a more flexible doctrinal tool, the application of which depends on the nature of the personal status concerned and the degree to which non-recognition affects fundamental rights. While the preservation of member states' regulatory autonomy remains a central element of the ECJ's reasoning, its limits are increasingly defined by the need to ensure the continuity of personal status and the effective protection of fundamental rights in cross-border situations. This confirms that the functional approach to recognition, as identified in this paper, operates as a coherent methodological framework in the case law of the ECJ, while allowing for variation in its intensity depending on the nature of the personal status and the degree of interference with fundamental rights.

5. CONCLUSION

The development of European case law in the field of cross-border family relationships demonstrates the gradual emergence of a functional approach to the recognition of family relationships as a coherent methodological framework in the case law of both the ECtHR and the ECJ. This approach is based on a clear distinction between the non-recognition of a particular family law institution as such and the obligation to recognise its legal effects to the extent necessary to protect fundamental rights and to ensure the continuity of personal status in cross-border situations. The analysis of the case law shows that both European courts, despite operating within different normative frameworks, converge in limiting the extent to which member states may rely on national autonomy and public policy where the non-recognition of family relationships would undermine fundamental aspects of individual identity, legal certainty, and the effective enjoyment of rights.

¹¹¹ See *Cupriak-Trojan*, *op. cit.* in fn. 109, paras. 1–77.

In this respect, particular importance is attached to the position of the child, whose rights, especially the right to identity and legal certainty, play a decisive role in determining the limits of state discretion.

In the case law of the ECJ, this approach is most clearly reflected in the judgments in *Coman* and *Pancharevo*, and further developed in more recent case law. While the ECJ consistently preserves the regulatory autonomy of member states in the field of family law, it imposes an obligation to recognise the legal effects of personal status lawfully acquired in another member state where this is necessary to ensure the effective exercise of rights derived from EU law. The scope of this obligation is not uniform, but varies depending on the nature of the personal status and the degree of interference with fundamental rights, as illustrated by the distinction between cases concerning family relationships and those concerning personal identity. This confirms that the functional approach to recognition operates as a flexible doctrinal tool, capable of adapting to the specific circumstances of each case while maintaining a consistent methodological core. At the same time, it reflects a gradual shift in European case law from a formal understanding of recognition towards an approach focused on the concrete legal effects of personal status and their impact on fundamental rights.

From the perspective of private international law, this development may be understood in light of the concept of the attenuated effect of public policy (*effet atténué*). While public policy remains a legitimate ground for limiting the recognition of foreign legal relationships, its application is increasingly restricted in cross-border situations where the refusal of recognition would disproportionately interfere with fundamental rights. In such cases, public policy does not operate as an absolute barrier, but rather as a flexible corrective mechanism, allowing for the recognition of certain legal effects of a personal status without requiring the full acceptance of the underlying institution within the national legal order. The functional approach to recognition can therefore be understood as reflecting, to a significant extent, the logic of the attenuated effect of public policy, reconciling the need to preserve the fundamental values of national legal systems with the imperative of ensuring the effective protection of fundamental rights and the continuity of personal status within the European legal space. At the same time, this comparison should not be understood as implying a complete equivalence between the two concepts, but rather as indicating a functional similarity in their operation in cross-border situations. Although it does not lead to the unification of family law at the European level, it provides a stable and adaptable framework for addressing the challenges posed by increasingly complex cross-border family situations. In this sense, the functional approach does not merely resolve individual cases, but contributes to the gradual shaping of a common European understanding of the limits of state autonomy in the field of personal status. Its further development will depend on the Court's ability to

maintain this balance in increasingly complex cross-border situations, particularly in areas where fundamental rights and national identity remain in structural tension.

REFERENCES

BOOKS AND ARTICLES

1. Bouček, V., *European Private International Law in the European Integration Process and Selected Issues of the Applicable Law*, Official Gazette, Zagreb 2021.
2. Corneloup, S.; Heiderhoff, B.; Honorati, C. (eds.), *Private International Law in a Context of Increasing International Mobility: Challenges and Potential*, Study for the JURI Committee, European Parliament, 2017.
3. De Groot, D. A. J. G., *Special Report: EU Law and the Mutual Recognition of Parenthood between Member States: The Case of V.M.A. v Stolichna obshtina*, RSCAS/GLOBALCIT Special Report, Robert Schuman Centre for Advanced Studies, European University Institute, No. 1/2021., p. 1–21.
4. European Parliament, *Cross-Border Legal Recognition of Parenthood in the EU*, Policy Department for Citizens' Rights and Constitutional Affairs, PE 746.632, 2023.
5. Fenton-Glynn, C., *International Surrogacy before the European Court of Human Rights*, *Journal of Private International Law*, Vol. 13, No. 3/2017., p. 546–567.
6. Frattone, C., *Same-sex Spouses' Rights in the ECJ's Coman Case*, *Roma Tre Law Review*, No. 2/2019., p. 303–315.
7. Garayova, L., *Parenthood without Borders: Judicial Cooperation for Cross-Border Family Security in the EU*, *EU and Comparative Law Issues and Challenges (ECLIC)*, No. 9/2025., p. 326–347.
8. Gyenyey, L., *Same Sex Couples' Right to Free Movement in Light of Member States' National Identities: The Legal Analysis of the Coman Case*, *Iustum Aequum Salutare*, Vol. 14, No. 2/2018., p. 149–171.
9. Hlača, N., *Personal Status of Citizens in the European Union*, in: Bodiřoga-Vukobrat, N.; Hlača, N.; Hrabar, D. (eds.), *European Family Law*, Official Gazette, Zagreb 2013.
10. Kochenov, D.; Belavusau, U., *Same-sex Spouses in the EU after Coman: More Free Movement, but What about Marriage?*, *EUI Working Paper LAW*, No. 3/2019., p. 1–18.

11. Lagarde, P., *Recognition and Registration of Civil Status Documents in Cross-Border Cases*, Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Brussels 2010.
12. Luku, H., *The Supreme Administrative Court of Bulgaria's Final Decision in the Pancharevo Case: Bulgaria Is Not Obligated to Issue Identity Documents for Baby S.D.K.A. as She Is Not Bulgarian (but Presumably Spanish)*, *Conflict of Laws*, 2023., p. 1–5.
13. Majstorović, I., *Family Law as Diversity in Unity: The European Union and Croatia*, in: Bodiřoga-Vukobrat, N.; Hlaća, N.; Hrabar, D. (eds.), *European Family Law*, Official Gazette, Zagreb 2013.
14. Marinkás, G., *Some Remarks on the CJEU's 'Pancharevo' Decision with Special Regard to the Nexus between the Primacy of EU Law and the National Identity of Member States*, *Law, Identity and Values*, Vol. 3, No. 1/2023., p. 177–201.
15. Palazzo, N., *Functional Recognition and Polyamory: Glitters and Hard Truths in the O'Neill Judgment*, *Journal of Social Welfare and Family Law*, Vol. 46, No. 2/2024., p. 187–207.
16. Rijpmma, J. J., *You Gotta Let Love Move: ECJ 5 June 2018, Case C-673/16, Coman, Hamilton, Accept v Inspectoratul General pentru Imigrări*, *European Constitutional Law Review*, Vol. 15, No. 2/2019., p. 234–339.
17. Sajko, K., *Private International Law*, 5th ed., Official Gazette, Zagreb 2009.
18. Scherpe, J. M., *Epilogue to the Family in EU Law – Is there a European Family Law?*, in: Part IV – The EU Family in Internal and External Crises, Cambridge University Press, 2024.
19. Shuilleabhain, M. N., *Surrogacy, System Shopping, and Article 8 of the European Convention on Human Rights*, *International Journal of Law, Policy and the Family*, Vol. 33, No. 1/2019., p. 104–122.
20. Trabucchi, A., *Istituzioni di diritto civile*, 27th ed., Cedam, Padova 1985.
21. Tryfonidou, A., *The Cross-Border Recognition of Changes in the Legal Sex of Transgender Persons: The Landmark Court of Justice Ruling in the Mirin Case*, *European Constitutional Law Review*, Cambridge University Press, 2025., p. 333–355.
22. Tryfonidou, A., *The ECJ Recognises the Right of Same-Sex Spouses to Move Freely between EU Member States: The Coman Ruling*, *European Law Review*, Vol. 44, No. 5/2019., p. 1–17.

LEGAL ACTS

1. Charter of Fundamental Rights of the European Union, OJ C 202/389, 7. 6. 2016.

2. Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States, amending Regulation (EEC) No. 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC, OJ L 158, 30. 4. 2004.
3. European Convention for the Protection of Human Rights and Fundamental Freedoms, Official gazette – International Treaties, No. 18/1997, 6/1999, 14/2002, 13/2003, 9/2005, 1/2006, 2/2010, 13/2017.
4. Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents, 5 October 1961, Official Gazette of the FPRY, MU No. 10/62; Official gazette – International Treaties, No. 4/4, 11/11.
5. Regulation (EU) 2016/1191 of the European Parliament and of the Council of 6 July 2016 on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents in the European Union and amending Regulation (EU) No. 1024/2012, OJ L 200, 26. 7. 2016.
6. Treaty on European Union, OJ C 202, 7.6.2016.
7. Treaty on the Functioning of the European Union (consolidated version), OJ C 202/49, 7. 6. 2016.

CASE LAW

1. Coman and Others v Inspectoratul General pentru Imigrări and Ministerul Afacerilor Interne, Case C-673/16, Judgment of 5 June 2018.
2. V.M.A. v Stolichna obshtina, rayon "Pancharevo", Case C-490/20, Judgment of 14 December 2021.
3. Labassee v. France, Application No. 65941/11, Judgment of 26 June 2014.
4. Mennesson v. France, Application No. 65192/11, Judgment of 26 June 2014.
5. Mirin, Case C-4/23, Judgment of 4 October 2024.
6. Cupriak-Trojan, Case C-713/23, Judgment of 5 December 2024.

NETWORK RESOURCES

1. European Family Law (PIL), Max-EuP 2012, Max Planck Encyclopedia of European Private Law, available at: <https://www.mpipriv.de/1417957/20211102-max-eup2012>
2. Functional Recognition of Same-sex Parenthood for the Benefit of Mobile Union Citizens – Brief Comments on the CJEU's Pancharevo Judgment, available at: <https://capil.org/2022/02/03/functional-recognition-of-same-sex->

parenthood-for-the-benefit-of-mobile-union-citizens-brief-comments-on-the-
cjeus-pancharevo-judgment/

UDK: 004.8 : 004.056
004.8 : 342.7
004.8 : 342.727
004.738.5 : 34 (094.5)
Preliminary communication

Hedvig Szabó, PostDoc researcher

Deák Ferenc Faculty of Law and Political Sciences, Széchenyi István University, Hungary

E-mail address: szabo.hedvig@sze.hu

ORCID-ID: 0009-0000-8403-8943

LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE- BASED DISINFORMATION AND DEEPPAKE TECHNOLOGIES IN THE EUROPEAN UNION PROTECTION OF DEMOCRATIC ELECTORAL PROCESSES AND THE BALANCE WITH FREEDOM OF SPEECH*

ABSTRACT

Artificial intelligence-generated disinformation, including deepfake technologies, poses unprecedented challenges to democratic processes and electoral integrity in the European Union. This study examines the evolving legal framework regulating AI-based disinformation detection and content moderation, with particular attention to the tension between protecting democratic functioning and fundamental rights, namely freedom of expression. The analysis situates these regulatory developments within the broader context of the European approach to digital transformation, taking into account emerging risks associated with artificial intelligence technologies. The research examines three main dimensions of the regulatory environment. First, it analyzes substantive legal instruments addressing AI-generated disinformation, including the Digital Services Act (DSA), the Artificial Intelligence Act (AI Act), and the European Democracy Action Plan, evaluating their coherence and effectiveness in responding to technologically sophisticated manipulation techniques. Second, it examines the institutional architecture of implementation, particularly the role of national authorities, platform responsibilities, and the emerging framework of co-regulation between public and private actors. Third, it assesses the fundamental rights implications of automated content moderation systems, focusing on the risks of over-removal, algorithmic bias, and chilling effects on legitimate political discourse.

Keywords: *disinformation; artificial intelligence; Digital Services Act; deepfake; freedom of speech*

1. INTRODUCTION

The digital age has fundamentally transformed the nature of political communication and the dynamics of shaping democratic public opinion. Unlike the traditional media environment, where gatekeepers and editorial standards provided a certain filtering mechanism, online platforms have enabled the immediate and global dissemination of information with virtually no oversight. This democratization has brought many positive changes while also creating new vulnerabilities that disinformation campaigns can exploit.¹

The rapid development of artificial intelligence technologies, particularly in the area of generative AI and deepfake capabilities, has exponentially increased the potential impact of disinformation. Deepfake technology creates synthetic media that convincingly depicts real individuals saying or doing things they never actually said or did. University College London has identified deepfake technology as one of the most significant societal threats of our time, blurring the line between reality and fiction, raising serious concerns regarding privacy, ethical implications, and security threats.²

The European Union has developed the world's first comprehensive regulatory framework to address these challenges, which includes the Digital Services Act (DSA), the Artificial Intelligence Act (AI Act), the Regulation on the Transparency of Political Advertising, and the European Democracy Action Plan. Together, these regulatory instruments apply a risk-based approach that attempts to balance the protection of democratic institutions with respect for freedom of expression and the right to access information.³

This study goes beyond the existing literature by examining the EU's regulatory instruments on disinformation and artificial intelligence not merely in isolation, but within an explicitly electoral and fundamental rights-focused interpretive framework. While most research on the Digital Services Act (DSA) and the Artificial Intelligence Act (AI Act) primarily concentrates on technology-neutral risk management logic, market compliance issues, or general fundamental rights impacts, this study examines the specific challenges that AI-based disinformation

* This paper was supported by the STARTING_25 funding scheme of the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund.

¹ Vosoughi, S., Roy, D., Aral, S., *The spread of true and false news online*, Science, Vol. 359, No. 6380, 2018, p. 1146.

² Caldwell, M., Andrews, J. T. A., Tanay, T., Griffin, L. D., *AI-enabled future crime*, Crime Science, Vol. 9, No. 1, 2020, Article 14.

³ Senftleben, M., *Guardians of the UGC galaxy*, JIPITEC, Vol. 14, No. 3, 2023, p. 270.

- particularly deepfake technologies - pose to the integrity of democratic electoral processes, and within what constitutional boundaries the handling of these challenges can remain legitimate in the EU fundamental rights system.

The novelty of the research lies in its integrated connection of the imperative to protect electoral integrity, the structural risks arising from the operation of automated content moderation systems, and the EU model of co-regulation as the dominant paradigm of legislative intervention. The study argues that strengthening democratic resilience is not solely a matter of suppressing disinformation content, but is equally dependent on institutional and technological decisions that determine the proportionality, transparency, and remedial guarantees of fundamental rights restrictions. Through this approach, the study contributes to the discourse on interpreting the DSA and AI Act by highlighting that the handling of AI-based disinformation in the electoral context becomes one of the EU legal system's most sensitive fundamental rights test areas in the digital age.

2. THEORETICAL AND CONCEPTUAL FRAMEWORKS

2.1. Conceptual Definition of Disinformation

Precise definition of the concept of disinformation is fundamental to the legitimacy of regulatory interventions. The literature and EU documents generally distinguish disinformation (intentionally disseminated false or misleading information), misinformation (unintentional dissemination of false information), and malinformation (real information disseminated with harmful intent). The EU approach primarily focuses on disinformation, which it defines as verifiably false or misleading information created, disseminated, and published for economic gain or to deliberately deceive the public, and which is likely to cause public harm.⁴

It is important to emphasize that disinformation itself does not necessarily constitute illegal content. Recital 84 of the DSA preamble specifically points out that very large online platforms must also pay attention to information that is not illegal but contributes to systemic risks as defined in this regulation, including misleading or deceptive content, including disinformation. This distinction is of central importance to understanding the constitutional limits of regulation, as

⁴ European Commission, *Tackling online disinformation: a European approach*, COM(2018) 236 final, 2018.

restricting freedom of expression requires greater justification in the case of non-illegal content.⁵

2.2. Deepfake Technology and Its Legal Challenges

According to Article 3(60) of the AI Act, deepfake means AI-generated or manipulated image, audio, or video content that depicts existing persons, objects, places, entities, or events and appears deceptively authentic or real to a person. This definition goes beyond the depiction of persons and includes objects, organizations, and events, recognizing that deepfake technology can be used not only for deceptive depictions of individuals but also of institutions.⁶

The availability and sophistication of deepfake technology has increased dramatically in recent years. In 2023, a 3000% increase in deepfake fraud attempts was recorded, while during the 2024 election year, the use of deepfakes for political purposes was documented in numerous countries. In Slovakia, AI-generated audio recordings spread just days before the 2023 elections, falsely depicting a liberal candidate discussing election fraud. In India's 2024 general elections, deepfakes depicting celebrities criticizing the prime minister went viral on WhatsApp and YouTube.⁷

2.3. Theoretical Foundations of Fundamental Rights Balance

The tension between combating disinformation and protecting freedom of expression is one of the most complex issues in fundamental rights doctrine. According to the consistent practice of the European Court of Human Rights (ECtHR), freedom of expression is one of the essential foundations of a democratic society, which applies to all information and ideas, including those that offend, shock, or disturb. However, this broad protection is not absolute: Article 10(2) of the European Convention on Human Rights allows restrictions provided

⁵ Husovec, M., *The Digital Services Act's red line: What the Commission can and cannot do about disinformation*, Journal of Media Law, Vol. 16, No. 1, 2024, p. 48.

⁶ Pawelec, M., *Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions*, Digital Society, Vol. 1, No. 2, 2022, Article 19.

⁷ Roy, E., Laskar, K. A., Reyaz, M., *Retroactive gatekeepers: Fact-checkers, electoral disinformation, and audience engagement in India*, Emerging Media, Vol. 3, No. 4, 2025, p. 585.

⁸ Macaulay, T., *Deepfake fraud attempts are up 3000% in 2023 - here's why*, The Next Web, 15 November 2023.

they are prescribed by law, serve legitimate aims, and are necessary in a democratic society.⁹

Article 11 of the EU Charter of Fundamental Rights provides similar protection, but in the EU context, the practice of the Court of Justice of the European Union (CJEU) is also of decisive importance. In Case C-401/19 Poland v. Parliament and Council (2022), the CJEU specifically addressed the relationship between online content moderation and freedom of expression, finding that preventive filtering obligations restrict an important means of disseminating online content and thus constitute a restriction of Article 11 of the Charter. At the same time, the Court upheld the justifiability of such restrictions with appropriate safeguards.

3. EU REGULATORY FRAMEWORK

3.1. Digital Services Act (DSA)

Regulation (EU) 2022/2065, the Digital Services Act (DSA), became fully applicable in the EU in February 2024 and is the world's first comprehensive online safety legislation applying a systematic approach to a wide range of online services and risks. The regulation aims to create a safe, predictable, and reliable online environment that promotes innovation while protecting fundamental rights enshrined in the EU Charter of Fundamental Rights, such as freedom of expression and information or non-discrimination.¹⁰

The DSA applies a multi-layered regulatory approach: it sets basic obligations for all services, enhanced obligations for online platforms, and the strictest requirements for very large online platforms (VLOPs) and very large online search engines (VLOSEs). VLOPs are those platforms whose average monthly active users in the Union reach or exceed 45 million. In April 2023, the European Commission designated the first 17 VLOPs, including Facebook, Instagram, LinkedIn, Snapchat, TikTok, Twitter (now X), and YouTube platforms, as well as 2 VLOSEs.¹¹

⁹ Gerards, J., *How to improve the necessity test of the European Court of Human Rights*, International Journal of Constitutional Law, Vol. 11, No. 2, 2013, p. 467.

¹⁰ Ó Fathaigh, R., Buijs, D., van Hoboken, J., *The regulation of disinformation under the Digital Services Act*, Media and Communication, Vol. 13, 2025.

¹¹ European Commission, *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*, IP/23/2413, 25 April 2023.

Article 34 of the DSA requires VLOPs to conduct annual risk assessments regarding systemic risks arising from the design, functioning, and use of their services. Under Article 35, platforms must take appropriate, proportionate, and effective risk mitigation measures. Disinformation is specifically included among the systemic risks that service providers must address, although the regulation emphasizes that risk mitigation measures do not necessarily mean content removal - demonetization, warning labels, or fact-checking references may also be applied.¹²

In February 2025, the European Commission and the European Board for Digital Services approved the integration of the Code of Practice on Disinformation into the DSA framework. From July 1, 2025, the Code will enjoy the status of a code of conduct under the DSA, meaning that the commitments contained therein become auditable and serve as a relevant reference point in assessing DSA compliance. This step makes the previously voluntary self-regulatory tool part of the legal framework, potentially with enforcement consequences for non-compliant platforms.¹³

3.2. Artificial Intelligence Act (AI Act)

Regulation (EU) 2024/1689, the AI Act, entered into force in August 2024 and is the world's first comprehensive AI regulation. The regulation applies a risk-based approach: it prohibits manipulative and exploitative AI systems, sets strict requirements for high-risk systems, and prescribes transparency obligations for certain AI applications, including systems generating deepfakes.¹⁴

Article 50 of the AI Act establishes specific transparency obligations for deepfakes. Providers of AI systems generating synthetic audio, image, video, or text content must ensure that the outputs are marked in machine-readable format and are recognizable as artificially generated or manipulated. Additionally, users employing deepfakes are obliged to publicly disclose that the content is artificially generated or manipulated. This transparency obligation does not apply to use authorized for the detection, prevention, or investigation of criminal offenses.¹⁵

¹² Husovec, M., *The Digital Services Act's red line*, *op. cit.*, note 6, p. 49.

¹³ Mündges, S., Park, K., *But did they really? Platforms' compliance with the Code of Practice on Disinformation in review*, 2024.

¹⁴ Laux, J., Wachter, S., Mittelstadt, B., *Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk*, *Regulation & Governance*, Vol. 18, No. 1, 2024, p. 5.

¹⁵ Łabuz, M., *op. cit.*, note 3.

It is important to note that the AI Act does not completely prohibit deepfakes. Instead, it imposes strict transparency requirements on both providers and users. The regulation's full applicability is due from August 2, 2026, although certain provisions - such as obligations regarding prohibited AI practices and AI literacy - entered into force earlier. In December 2025, the Commission published the first draft of a code of practice on marking and labeling AI-generated content, providing practical guidance on watermarking, metadata, and other technical measures.¹⁶

3.3. Regulation on Transparency of Political Advertising

Regulation (EU) 2024/900 on the transparency and targeting of political advertising (TTPA) entered into force on April 9, 2024, with most provisions applicable from October 10, 2025. The regulation aims to contribute to the proper functioning of the internal market for political advertising and to open, fair political debate, addressing concerns about information manipulation and foreign interference in elections.¹⁷

The regulation requires that political advertisements be clearly marked as political advertisements and provide information about who financed them, which election or referendum they relate to, and whether targeting or ad delivery techniques were used. Targeted political advertising in an online environment is only permitted under strict conditions: data must be collected from the data subject and may only be used if the data subject has given explicit and separate consent for their use for political advertising purposes. Special categories of data - such as data relating to racial or ethnic origin or political opinions - cannot be used for profiling.¹⁸

To prevent foreign interference, it is prohibited to provide political advertising services to sponsors from third countries during the last three months before elections or referendums. In the event of violations, sanctions established by Member States may reach up to 6% of the service provider's annual worldwide turnover. The regulation also establishes a public European repository of online

¹⁶ Meding, L., Burchardi, A., Veale, M., *What constitutes a deep fake? The blurry line between legitimate processing and manipulation under the EU AI Act*, Proceedings of the ACM Symposium on Computer Science and Law, ACM, 2025.

¹⁷ Nikiforov, L., *Transparency in targeting of political advertising: Challenges remain*, SSRN Working Paper, 1 November 2024.

¹⁸ Stephenson, R., Rinceanu, J., Bovermann, M. A., *Regulating political advertising in the EU: Transparency without accountability*, Euclid, 2025(1), p. 91.

political advertising, where all online political advertisements will be publicly accessible.

3.4. European Democracy Action Plan

The European Commission presented the European Democracy Action Plan (EDAP) in December 2020, which announced further steps, including legislative measures, as a non-legislative initiative. The Action Plan has three main pillars: protecting the integrity of elections and promoting democratic participation, strengthening media freedom and media pluralism, and combating disinformation, foreign interference, and information influence operations.¹⁹

Within the framework of the Action Plan, the EU has intensified its response to disinformation threats both domestically and internationally. This includes establishing an operational mechanism through the European Cooperation Network on Elections, strengthening the Code of Practice on Disinformation, and supporting civil society and media freedom. The plan also sets out measures to protect journalists from abusive lawsuits (SLAPP) and to strengthen transparency in media ownership.²⁰

4. INSTITUTIONAL ARCHITECTURE OF IMPLEMENTATION

4.1. Multi-level Implementation Mechanisms

The DSA creates a multi-level enforcement system in which national-level Digital Services Coordinators (DSCs) and the European Commission have shared competences. Member States were obliged by the February 2024 deadline to designate an independent regulatory authority as a DSC, which is responsible for enforcing the rules on intermediary services, hosting services, and non-VLOP platforms in their territory. The designated DSCs have different backgrounds - some are new bodies, others are existing communication, media regulatory, consumer protection, or competition authorities.²¹

¹⁹ European Commission, *European Democracy Action Plan*, COM(2020) 790 final, 2020.

²⁰ Haapala, I., Roch, C., *EU democratic resilience in times of information warfare: A study of the European Democracy Action Plan*, European Foreign Affairs Review, Vol. 30, No. 1, 2025, p. 85.

²¹ Rangoni, B., Thatcher, M., *National de-delegation in multi-level settings: Independent regulatory agencies in Europe*, Governance, Vol. 36, No. 1, 2023, p. 85.

Regarding the supervision of VLOPs and VLOSEs, the European Commission acts as the exclusive enforcement authority. In 2023, the Commission established the European Centre for Algorithmic Transparency (ECAT), which supports enforcement efforts. The Commission has initiated several proceedings against major platforms, including against Meta, TikTok, and X (formerly Twitter), due to concerns that they are not complying with the DSA's requirements on electoral integrity. In March 2024, the Commission issued guidelines for VLOPs and VLOSEs on recommended measures to mitigate systemic risks affecting electoral processes.²²²³²⁴

4.2. The Co-regulation Model

The EU's approach to addressing disinformation is based on a co-regulation model that combines mandatory legal requirements and industry self-regulatory initiatives. Article 45 of the DSA allows for the development of codes of conduct serving specific public interest objectives. The Code of Practice on Disinformation, strengthened in 2022, was specifically designed to be recognized as a code of conduct under the DSA, which was realized in 2025.²⁵

Signatories to the Code - including online platforms, search engines, the advertising industry, fact-checking organizations, and civil society organizations - commit to implementing various measures, such as diverting advertising revenue from disinformation content, ensuring transparency in political advertising, providing users with tools and features to recognize disinformation, and ensuring researchers' access to data. This model provides flexibility for platforms in choosing how to comply while establishing common standards and control mechanisms. However, due to the Code's voluntary nature, platforms do not face meaningful sanctions for non-compliance with commitments, and enforcement is often fragmented and performative.²⁶

²² Sundorph, E., *European Centre for Algorithmic Transparency (ECAT): Issue 3*, Publications Office of the European Union, 2024.

²³ Miller, G., *EU tests DSA with investigative proceedings against Musk's X*, TechPolicy Press, 19 December 2023.

²⁴ Broughton Micova, S., Schnurr, D., *Systemic risk in digital services: Benchmarks for evaluating the management of risks to electoral processes*, CERRE, 2024.

²⁵ Oleart, A., Bouza García, L., *From self to co-regulation in the EU's approach to disinformation*, International Review of Public Policy, Vol. 7, No. 2, 2025, p. 240.

²⁶ Shattock, E., *Self-regulation 2.0? A critical reflection of the European fight against disinformation*, Harvard Kennedy School Misinformation Review, 2021.

5. FUNDAMENTAL RIGHTS IMPLICATIONS AND RISKS

5.1. Risks of Algorithmic Content Moderation

A natural consequence of the systemic risk assessment and mitigation required by the DSA is that platforms increasingly rely on algorithmic systems for large-scale content moderation. However, this development carries significant fundamental rights risks. According to a 2024 study by Vanderbilt University's Future of Free Speech research institute, platforms may over-moderate content to avoid DSA fines, which can lead to unjustified removal of lawful content.²⁷

One of the most serious problems with algorithmic content moderation is inconsistency and arbitrariness. Research has shown that different machine learning models can produce different classification results for the same content, leading to a phenomenon called predictive multiplicity. This means that the restriction of freedom of expression - which theoretically requires justification - may depend on the technical decision of model selection rather than objective legal criteria. The opacity of such arbitrary decisions poses a threat to fundamental freedoms, as restrictions must be justifiable.²⁸

The reinforcement of bias is another concern. Research has documented that algorithmic content moderation disproportionately affects certain social groups. Messages containing minority identity markers (e.g., Arab, Black, LGBTQ+), explicit profanity, or specific racial and ethnic dialects (e.g., African American English) are more likely to be classified as toxic, regardless of their communication context. The EU Fundamental Rights Agency expressed concern in 2023 that large amounts of misogyny and racism bypass content moderation systems, while algorithms are prone to errors and may ultimately popularize online hatred over time.²⁹

²⁷ Alkiviadou, N., *Platform liability, hate speech and the fundamental right to free speech*, Information & Communications Technology Law, Vol. 34, No. 2, 2024, p. 3.

²⁸ Gomez, J. F., Machado, C. V., Paes, L. M., Calmon, F. P., *Algorithmic arbitrariness in content moderation*, Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency, 2024, p. 2235.

²⁹ EU Fundamental Rights Agency (FRA), *Online content moderation: Current challenges in detecting hate speech*, <https://fra.europa.eu/en/publication/2023/online-content-moderation>, 29 November 2023.

5.2. Over-removal and Chilling Effect

The phenomenon of over-removal, when lawful content is mistakenly removed, is particularly concerning in the context of political speech. The ECtHR has consistently emphasized that political expression enjoys enhanced protection and should be evaluated from the perspective of its contribution to democratic debate. However, automated filters are often unable to understand context and nuance, which can lead to mistaken removal of legitimate political criticism.³⁰

The concept of chilling effect has long been recognized in freedom of expression jurisprudence. This phenomenon occurs when individuals introduce voluntary restrictions on their expressions out of fear of illegal proceedings or sanctions, even if their expression would actually be protected. In the context of online content moderation, the chilling effect occurs when users avoid discussing certain topics or expressing opinions because they fear their content will be removed or their accounts suspended. Multi-stage complaint and dispute resolution processes can frustrate users and lead them to abandon well-founded claims for restoration of their uploads.³¹

5.3. Relevant Case Law of the CJEU and ECtHR

The CJEU's judgment in Case C-18/18 *Glawischnig-Piesczek v. Facebook Ireland* (2019) is one of the landmark decisions on the relationship between content moderation and freedom of expression. The Court ruled that when a court orders the removal of an unlawful post, it may also order the removal of identical content and content that is equivalent in content. This judgment raised concerns about the use of automated filters, which can lead to context-independent removals.³²

In Case C-401/19 *Poland v. Parliament and Council* (2022), the CJEU's Grand Chamber examined the constitutionality of Article 17 of the Copyright Directive from the perspective of freedom of expression. The Grand Chamber found that preventive filtering obligations restrict an important means of disseminating online content, thereby constituting a restriction of Article 11 of the Charter.

³⁰ Gorwa, R., Binns, R., Katzenbach, C., *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*, Big Data & Society, Vol. 7, No. 1, 2020, p. 5.

³¹ Are, C., *'Dysfunctional' appeals and failures of algorithmic justice in Instagram and TikTok content moderation*, Information, Communication & Society, Vol. 28, No. 11, 2025, p. 2000.

³² Keller, D., *Facebook filters, fundamental rights, and the CJEU's Glawischnig-Piesczek ruling*, GRUR International, Vol. 69, No. 6, 2020, p. 617.

However, the Court upheld the justifiability of the restriction, emphasizing that Member States must provide appropriate safeguards for the protection of freedom of expression, including ensuring that platforms only block manifestly unlawful content.³³

The ECtHR's judgment in *Sanchez v. France* (2023) raised new questions regarding social media content moderation. The Grand Chamber found that a politician's criminal liability for hate speech comments written by others on their Facebook page did not violate Article 10 of the Convention because the politician did not exercise appropriate vigilance regarding the comments. This judgment raised concerns that it holds public figures responsible for others' content, which may encourage them to preventively restrict commenting options.³⁴

6. SPECIFICITIES OF THE ELECTORAL CONTEXT

6.1. The Imperative of Protecting Electoral Integrity

The protection of electoral integrity is a legitimate public interest objective that can justify certain restrictions on freedom of expression. The United States Supreme Court in *Burson v. Freeman* (1992) recognized that protecting the integrity of elections is a compelling state interest that can justify restrictions - such as prohibiting campaign activities near polling places. However, in other cases, such as *McIntyre v. Ohio Elections Commission* (1995), the Court found that certain electoral rules go too far and violate the First Amendment.

In the EU context, the DSA's electoral guidelines issued in March 2024 provide recommendations for VLOPs and VLOSEs to mitigate systemic risks affecting electoral processes before, during, and after elections. While not legally binding, the guidelines clarify the DSA text and provide practical, current examples of how services can meet their risk mitigation obligations under the DSA. They pay particular attention to measures on online political advertising and generative AI.³⁵

6.2. The Impact of Deepfakes on Elections: Empirical Experience

³³ Senftleben, M., *Guardians of the UGC galaxy*, JIPITEC, Vol. 14, No. 3, 2023, p. 270.

³⁴ Husovec, M., Grote, T., et al., *Grand confusion after Sanchez v. France*, Common Market Law Review, 2024.

³⁵ Broughton Micova, S., Schnurr, D., *op. cit.*, note 25.

During the 2024 super election year, when more than half of the world's population participated in elections, numerous cases documented the use of deepfakes for electoral purposes. The most widely cited case occurred before the January 2024 New Hampshire primary, when AI-generated robocalls - imitating President Joe Biden's voice - called on voters not to vote. The Federal Communications Commission subsequently declared robocalls containing AI-generated voices illegal.³⁶

However, it is important to nuance the assessment of the deepfake threat. The Alan Turing Institute's study found that AI-based disinformation did not actually have a significant impact on 2024 election results in the United Kingdom and EU. While there were viral deepfakes, users amplifying the content generally came from a small number of people identifying with ideological narratives embedded in that content. In other words, the most controversial voices on platforms generally do not influence undecided voters.³⁷

The Brennan Center for Justice analysis pointed out that the long-term impact of deepfakes goes beyond immediate disinformation. The liar's dividend phenomenon means that the existence of deepfakes allows anyone - politicians, corporations, or other influential figures - to avoid accountability by questioning the authenticity of credible evidence. Over time, this uncertainty weakens democratic institutions, promotes alienation, and makes societies more vulnerable to manipulation.³⁸

7. CHALLENGES AND RECOMMENDATIONS

7.1. Challenges of Regulatory Coherence

Despite the EU's comprehensive regulatory architecture, significant challenges remain in ensuring coherent and effective implementation. Addressing potential overlaps and contradictions between the AI Act and DSA requires ongoing attention. For example, both regulations prescribe transparency obligations for AI-

³⁶ Federal Communications Commission, *Declaratory Ruling on AI-generated robocalls*, FCC 24-17, 8 February 2024.

³⁷ The Alan Turing Institute, *Turing event at the Houses of Parliament explores impact of AI disinformation on elections*, <https://www.turing.ac.uk/news/>, 30 January 2025.

³⁸ Schiff, K. J., Schiff, D. S., Bueno, N. S., *The liar's dividend: Can politicians claim misinformation to evade accountability?*, American Political Science Review, Vol. 118, No. 2, 2024, p. 650.

generated content but apply different terminology and approaches. Member States have different regulatory frameworks and implementation capacities, which can lead to uneven application.

The AI Act does not specify which regulatory authority should act as a supervisory body, so Member States must establish their own national sanction systems, which can lead to different enforcement practices. Some Member States - such as Spain - have created dedicated regulatory bodies to supervise AI developments, while others - such as France and Germany - do not yet have specific legislation or bodies for regulating artificial intelligence. This fragmentation may weaken the effectiveness of the EU-level response.³⁹

7.2. Technological Challenges

Despite the rapid development of deepfake detection technologies, significant technical limitations remain. Generative AI models are becoming increasingly sophisticated, while detection systems always struggle with a step behind. Current detection systems are particularly weak in identifying voice-based deepfakes, which are increasingly popular in electoral disinformation campaigns, as evidenced by the Slovak and United States cases.⁴⁰

Implementation of the watermarking and metadata requirements prescribed by the AI Act also poses challenges. Malicious actors may intentionally remove metadata and detection markings. Additionally, enforcement on global platforms - where content originates from and is directed to different jurisdictions - raises practical difficulties. Organizations cannot rely solely on upstream compliance; they need independent verification capabilities to identify synthetic content regardless of source or labeling status.⁴¹

7.3. Recommendations for Legislators and Platforms

Based on the research, the following recommendations can be formulated for effective and fundamental rights-compliant disinformation regulation. First,

³⁹ Future of Life Institute, *Overview of all AI Act national implementation plans*, <https://artificialintelligenceact.eu/national-implementation-plans>, 19 May 2025.

⁴⁰ Sharma, K., *AI voice cloning and deepfakes are here, and they are dangerous*, Scientific American, 15 January 2026.

⁴¹ Feltes, N., *Article 50 AI Act: Do the transparency provisions improve upon the Commission's draft?*, JIPITEC, Vol. 16, 2025, p. 230.

strengthening transparency obligations for algorithmic content moderation systems is necessary. Platforms should publicly make available descriptions of the main parameters of algorithmic decision-making, error rates, and breakdowns by affected user groups. This would enable independent researchers and regulators to identify patterns of bias and over-removal.

Second, strengthening human oversight requirements is essential, particularly regarding political content and electoral periods. The DSA requires ensuring human oversight in content moderation decisions, but further attention is needed to specify and monitor compliance with these requirements. In the case of political speech - where understanding context is critical - purely automated decision-making can be particularly problematic.

Third, ensuring effective remedial mechanisms for cases of erroneous removal is indispensable. Article 20 of the DSA requires platforms to establish internal complaint handling mechanisms, and Article 21 allows for out-of-court dispute resolution. However, evaluating the effectiveness of these mechanisms and strengthening them as needed is an ongoing task. Users must be provided with clear, prompt, and cost-free procedures to request restoration of their content.

Fourth, developing media literacy and critical thinking throughout society is of paramount importance. Technical and legal solutions alone are not sufficient; citizens need to be able to recognize disinformation and manipulated content. The European Democracy Action Plan rightly emphasizes supporting media literacy programs, and intensifying these efforts is warranted.

8. CONCLUSION

This study has provided a comprehensive analysis of the legal regulation of AI-based disinformation and deepfake technologies in the European Union, with particular attention to the protection of democratic electoral processes and respect for freedom of expression. The research findings indicate that the EU has developed a comprehensive regulatory architecture - through the DSA, AI Act, Regulation on the Transparency of Political Advertising, and the European Democracy Action Plan - representing the world's most advanced framework for addressing these challenges.

However, significant challenges remain in ensuring proportionate and fundamental rights-respecting implementation. Reliance on AI-based detection

systems introduces new risks of error and opacity that may undermine the very democratic values that regulation seeks to protect. The inconsistency and bias of algorithmic content moderation, the phenomenon of over-removal, and the chilling effect on political speech are all problems requiring ongoing attention and fine-tuning.

The study argues that effective disinformation governance requires not only robust legal frameworks but also transparency obligations for detection algorithms, meaningful human oversight, and effective remedial mechanisms for erroneous content removals. Finding the balance between protecting democratic institutions and respecting freedom of expression remains an ongoing challenge requiring constant dialogue and cooperation among regulators, platforms, civil society, and researchers.

The pace of technological development exceeds the adaptive capacity of regulation, necessitating a flexible, risk-based approach. The EU's co-regulation model - which combines mandatory legal requirements and industry self-regulatory initiatives - offers a promising approach, but its success depends on the quality of implementation and continuous review.

Ultimately, democratic resilience depends not only on legal and technical tools but also on society's overall media literacy, critical thinking, and commitment to democratic values. Legal regulation is an important tool, but it is not sufficient alone to protect the democratic public sphere in the digital age.

REFERENCES

BOOKS AND ARTICLES

1. Alkiviadou, N., *Platform liability, hate speech and the fundamental right to free speech*, Information & Communications Technology Law, Vol. 34, No. 2, 2024, pp. 1-11.
2. Are, C., *'Dysfunctional' appeals and failures of algorithmic justice in Instagram and TikTok content moderation*, Information, Communication & Society, Vol. 28, No. 11, 2025, pp. 1997-2014.
3. Broughton Micova, S., Schnurr, D., *Systemic risk in digital services: Benchmarks for evaluating the management of risks to electoral processes*, Centre for Regulation in Europe (CERRE), 2024.

4. Caldwell, M., Andrews, J. T. A., Tanay, T., Griffin, L. D., *AI-enabled future crime*, Crime Science, Vol. 9, No. 1, 2020, Article 14.
5. Feltes, N., *Article 50 AI Act: Do the transparency provisions improve upon the Commission's draft?*, JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law, Vol. 16, 2025, pp. 222-240.
6. Gerards, J., *How to improve the necessity test of the European Court of Human Rights*, International Journal of Constitutional Law, Vol. 11, No. 2, 2013, pp. 466-490.
7. Gomez, J. F., Machado, C. V., Paes, L. M., Calmon, F. P., *Algorithmic arbitrariness in content moderation*, Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (FAccT '24), ACM, 2024, pp. 2234-2253.
8. Gorwa, R., Binns, R., Katzenbach, C., *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*, Big Data & Society, Vol. 7, No. 1, 2020, pp. 1-15.
9. Haapala, I., Roch, C., *EU democratic resilience in times of information warfare: A study of the European Democracy Action Plan*, European Foreign Affairs Review, Vol. 30, No. 1, 2025, pp. 83-106.
10. Husovec, M., *The Digital Services Act's red line: What the Commission can and cannot do about disinformation*, Journal of Media Law, Vol. 16, No. 1, 2024, pp. 47-56.
11. Husovec, M., Grote, T., Mazhar, Y., Mikhaeil, C., Miñarro Escalona, H., Sinha Kumar, P., Sreenath, S., *Grand confusion after Sanchez v. France: Seven reasons for concern about Strasbourg jurisprudence on intermediaries*, Common Market Law Review, 2024.
12. Keller, D., *Facebook filters, fundamental rights, and the CJEU's Glawischnig-Piesczek ruling*, GRUR International, Vol. 69, No. 6, 2020, pp. 616-623.
13. Łabuz, M., *A teleological interpretation of the definition of deepfakes in the EU Artificial Intelligence Act*, Policy & Internet, 2025.
14. Laux, J., Wachter, S., Mittelstadt, B., *Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk*, Regulation & Governance, Vol. 18, No. 1, 2024, pp. 3-32.
15. Macaulay, T., *Deepfake fraud attempts are up 3000% in 2023 - here's why*, The Next Web, 15 November 2023.
16. Meding, L., Burchardi, A., Veale, M., *What constitutes a deep fake? The blurry line between legitimate processing and manipulation under the EU AI Act*, Proceedings of the ACM Symposium on Computer Science and Law, ACM, 2025.

17. Miller, G., *EU tests DSA with investigative proceedings against Musk's X*, TechPolicy Press, 19 December 2023.
18. Mündges, S., Park, K., *But did they really? Platforms' compliance with the Code of Practice on Disinformation in review*, , 2024.
19. Nikiforov, L., *Transparency in targeting of political advertising: Challenges remain*, SSRN Working Paper, 1 November 2024.
20. Ó Fathaigh, R., Buijs, D., van Hoboken, J., *The regulation of disinformation under the Digital Services Act*, Media and Communication, Vol. 13, 2025.
21. Oleart, A., Bouza García, L., *From self to co-regulation in the EU's approach to disinformation: The framing power of Big Tech business lobbies in the lead to the Digital Services Act*, International Review of Public Policy, Vol. 7, No. 2, 2025, pp. 235-256.
22. Pawelec, M., *Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions*, Digital Society, Vol. 1, No. 2, 2022, Article 19.
23. Rangoni, B., Thatcher, M., *National de-delegation in multi-level settings: Independent regulatory agencies in Europe*, Governance, Vol. 36, No. 1, 2023, pp. 81-103.
24. Roy, E., Laskar, K. A., Reyaz, M., *Retroactive gatekeepers: Fact-checkers, electoral disinformation, and audience engagement in India*, Emerging Media, Vol. 3, No. 4, 2025, pp. 582-600.
25. Schiff, K. J., Schiff, D. S., Bueno, N. S., *The liar's dividend: Can politicians claim misinformation to evade accountability?*, American Political Science Review, Vol. 118, No. 2, 2024, pp. 648-666.
26. Senftleben, M., *Guardians of the UGC galaxy: Human rights obligations of online platforms, copyright holders, member states and the European Commission under the CDSM Directive and the Digital Services Act*, JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law, Vol. 14, No. 3, 2023, pp. 264-289.
27. Shattock, E., *Self-regulation 2.0? A critical reflection of the European fight against disinformation*, Harvard Kennedy School Misinformation Review, 2021.
28. Sharma, K., *AI voice cloning and deepfakes are here, and they are dangerous*, Scientific American, 15 January 2026.
29. Stephenson, R., Rinceanu, J., Bovermann, M. A., *Regulating political advertising in the EU: Transparency without accountability*, Eucrium - European Law Forum: Prevention • Investigation • Prosecution, 2025(1), pp. 90-97.
30. Sundorph, E., *European Centre for Algorithmic Transparency (ECAT): Issue 3*, Publications Office of the European Union (E. A. Pena Fernandez, Ed.; JRC139131), 2024.

31. van Drunen, M., Helberger, N., Ó Fathaigh, R., *The beginning of EU political advertising law: Unifying democratic visions through the internal market*, International Journal of Law and Information Technology, Vol. 30, No. 4, 2022, pp. 424-445.
32. Vosoughi, S., Roy, D., Aral, S., *The spread of true and false news online*, Science, Vol. 359, No. 6380, 2018, pp. 1146-1151.

LEGAL RULES

1. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Official Journal of the European Union, L 277, 1-102.
2. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Official Journal of the European Union, L 2024/1689.
3. Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, Official Journal of the European Union, L 2024/900.
4. European Commission, Tackling online disinformation: a European approach (COM(2018) 236 final), 2018.
5. European Commission, European Democracy Action Plan (COM(2020) 790 final), 2020.
6. Federal Communications Commission, In the Matter of Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts (CG Docket No. 23-362, Declaratory Ruling, FCC 24-17), 8 February 2024.

COURT PRACTICE

1. Case C-18/18, Glawischnig-Piesczek v. Facebook Ireland, ECLI:EU:C:2019:821 (Court of Justice of the European Union, 3 October 2019).
2. Case C-401/19, Poland v. Parliament and Council, ECLI:EU:C:2022:297 (Court of Justice of the European Union, 26 April 2022).
3. Sanchez v. France, Application no. 45581/15 (European Court of Human Rights [Grand Chamber], 15 May 2023).

NETWORK RESOURCES

1. EU Fundamental Rights Agency (FRA), Online content moderation: Current challenges in detecting hate speech, <https://fra.europa.eu/en/publication/2023/online-content-moderation>, 29 November 2023.
2. Future of Life Institute, Overview of all AI Act national implementation plans, <https://artificialintelligenceact.eu/national-implementation-plans>, 19 May 2025.
3. The Alan Turing Institute, Turing event at the Houses of Parliament explores impact of AI disinformation on elections, <https://www.turing.ac.uk/news/turing-event-houses-parliament-explores-impact-ai-disinformation-elections>, 30 January 2025.

UDK: 004.738.5 : 34 (094.5)
341.24 : 615 (4-67
EU)(094.5)
Preliminary communication

Lisa Marie Breyer, PhD student
Faculty of Law, University of Vienna, Austria
E-mail: Lisa.marie.breyer@univie.ac.at
ORCID-ID: 0009-0004-0072-3302

THE PRESUMPTION OF CONFORMITY FOR MEDICAL AI UNDER THE AI ACT: STRUCTURAL LIMITS OF MDR CONFORMITY ASSESSMENT FOR CONTINUOUS-LEARNING GENETIC DIAGNOSTIC SOFTWARE

ABSTRACT

Continuous-learning deep-learning (DL) systems used in genetic diagnostics sit at the intersection of the EU Artificial Intelligence Act (AI Act), the Medical Device Regulation (MDR), and data protection law. Under Article 6(1) AI Act and Annex I, Section A, such systems qualify as high-risk AI systems where they constitute medical device software within the meaning of Article 2 MDR and are subject to third-party conformity assessment under the MDR. For Annex I systems, Article 43(3) channels conformity assessment through the MDR, while compliance with harmonised standards may give rise to a presumption of conformity under Article 42 AI Act. This article assesses whether MDR conformity assessment—predominantly ex ante and premised on stable device identities—provides an equivalent basis for that presumption when applied to continuously learning genetic diagnostic software. Doctrinal analysis of MDR classification (Annex VIII, Rule 11) and the conformity assessment routes (Annexes IX–XI) reveals a structural mismatch. MDR conformity assessment relies on snapshot-based technical documentation, verification/validation testing, and quality management systems that presuppose a fixed intended purpose and stable performance characteristics. While Annex IX offers procedural completeness through controlled change governance, it does not enable continuous substantive reassessment of evolving behaviour; Annex X and Annex XI reinforce type-based and unit-based verification logics that are difficult to reconcile with model-state evolution. The article demonstrates that, for continuous-learning genetic diagnostics, the MDR's conformity architecture may not be functionally equivalent to the AI Act's lifecycle-oriented risk logic, thereby limiting the reliability of the presumption of conformity in this domain.

Keywords: Artificial Intelligence Act, Medical Device Regulation, Presumption of Conformity, Continuous Learning Systems, Genetic Diagnostics

1. INTRODUCTION

Deep-learning (hereinafter: DL) systems in genetic diagnostics raise unprecedented legal, ethical, and technical challenges. Artificial Intelligence (hereinafter: AI) used for genetic analysis is governed by several regulatory frameworks at both European and national levels, including the Artificial Intelligence-Act (hereinafter: AI Act),¹ the Medical Device Regulation (hereinafter: MDR),² the General Data Protection Regulation (hereinafter: GDPR),³ and, for example, in Austria, the Genetic Technology Act (Gentechnikgesetz, hereinafter: GTG).⁴ These frameworks pursue distinct objectives⁵ and are structured around different regulatory logics,⁶ risk concepts,⁷ and enforcement mechanisms.⁸

The AI Act entered into force on 1 August 2024.⁹ Legal scholarship has established that a deep-learning model used for diagnosis qualifies as software, and accordingly, as a medical device within the meaning of the MDR.¹⁰ Consequently,

¹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 2024/1689 (hereinafter: AI Act).

² Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices (Medical Device Regulation), OJ L 2017/117 (hereinafter: MDR); Königshofer, W., Medical Device Law, in: Resch, R.; Wallner, F. (eds.), Handbook of Medical Law, 3rd ed., Manz, Vienna 2020, para. 23; European Commission, *Medical devices: Guidance document – Qualification and Classification of stand alone software (MEDDEV 2.1/6)*, July 2016, p. 9 *et seq.*, <https://ec.europa.eu/docsroom/documents/17921>, accessed 21 February 2026. This document is based on Directive 93/42/EEC; Annex II of the Council Resolution of 7 May 1985 on a new approach to technical harmonisation and standardisation (85/C 136/01), OJ C 1985/136, 1; Schneeberger, D., *Intelligente Medizinprodukte: Rechtsfragen am Schnittpunkt von DSGVO, MPVO und AI Act*, DaKo, 1/2024, p. 5 *et seq.*

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation), OJ L 2016/119 (hereinafter: GDPR); Herbst, T., *Regulierung intelligenter Medizinprodukte*, ZfPC, 2023, p. 246.

⁴ Genetic Technology Act (Gentechnikgesetz – GTG), Federal Law Gazette (BGBl) No 510/1994, as amended by BGBl I No 8/2022 (hereinafter: GTG).

⁵ Recitals 1, 8, 176 AI Act; Recital 1, 2, 101 MDR; Recital 170 GDPR.

⁶ Recital 26 AI Act; *European Commission*, Commission Notice – The ‘Blue Guide’ on the implementation of EU product rules 2022, OJ C 247, 29.6.2022, 9-13, 70-80.

⁷ Recitals 26, 27, 64-66, Article 4, 9 AI Act; Recitals 31-33, 58, 59, Article 1, 51, Annex VIII MDR; Recital 75, Article 35 GDPR.

⁸ Chapter IX Section 3 AI Act; Chapter VII MDR; Article 51 and 83 GDPR.

⁹ European Commission, AI Act enters into force, 1 August 2024, https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en, accessed 21 February 2026.

¹⁰ Article 2(1) MDR; Königshofer, W., *op. cit.* note 2, para. 23; European Commission, *Medical devices: Guidance document – Qualification and Classification of*

such software constitutes a high-risk AI system within the meaning of Article 6(1) of the AI Act,¹¹ while, at the same time, remaining subject to the applicable provisions of the GDPR.¹²

Deep-learning models introduce specific risks, including misdiagnosis, bias,¹³ performance uncertainty¹⁴ or unpredictable model behaviour.¹⁵ Their feedback loops¹⁶ and ability for continuous learning¹⁷ result in evolving neuronal network configurations¹⁸ that may interact with patient data in unforeseen ways. The AI Act seeks to address certain of these risks, *inter alia*, through the establishment of a risk management system¹⁹, specific technical requirements relating to feedback loops,²⁰ and conformity assessment obligations.²¹

stand alone software (MEDDEV 2.1/6), July 2016, p. 9 *et seq.*, <https://ec.europa.eu/docsroom/documents/17921>, accessed 21 February 2026. This document is based on Directive 93/42/EEC; Annex II of the Council Resolution of 7 May 1985 on a new approach to technical harmonisation and standardisation (85/C 136/01), OJ C 1985/136, 1.

¹¹ This analysis is based on Regulation (EU) 2024/1689 as adopted. At the time of writing, the European Commission has proposed amendments that would move medical devices governed by Regulation (EU) 2017/745 (MDR) from Annex I, Section A to Section B of the AI Act. Should such amendments be adopted, the direct applicability of certain high-risk AI system requirements may be modified pursuant to Article 2(2) AI Act. The structural question examined in this article—namely whether the MDR conformity architecture is conceptually capable of governing continuously learning systems—remains relevant irrespective of the final legislative configuration. See: <https://www.osborneclarke.com/insights/eu-mdr-and-ivdr-poised-remain-main-framework-medical-ai-draft-ai-interface-reforms>; <https://www.taylorwessing.com/en/insights-and-events/insights/2026/02/reform-der-mdr-und-ivdr>; <https://www.emergobyul.com/news/ec-requests-feedback-proposed-regulation-simplify-mdr-ivdr>.

¹² Article 2(7) AI Act; Herbst, T., *op. cit.* note 3, p. 246.

¹³ Zhang, A. *et al.*, Shifting Machine Learning for Healthcare from Development to Deployment and from Models to Data, *Nature Biomedical Engineering*, 6(12), 2022, p. 1343-1344. doi:10.1038/s41551-022-00898-y; Wang, X. *et al.*, Inconsistent Performance of Deep Learning Models on Mammogram Classification, *Journal of the American College of Radiology*, 17(6), 2020, p. 796-803. doi: 10.1016/j.jacr.2020.01.006.

¹⁴ Zhang *et al.*, *op. cit.* note 13, p. 1343; Gama, J. *et al.*, A Survey on Concept Drift Adaptation, *ACM Computing Surveys*, 46(4), 2014, p. 3-4, doi:10.1145/2523813.

¹⁵ Gama *et al.*, *op. cit.* note 14, p. 3-4.

¹⁶ Sculley, D. *et al.*, Hidden Technical Debt in Machine Learning Systems, *Advances in Neural Information Processing Systems*, 2015, p. 2506.

¹⁷ Goodfellow, I.; Bengio, Y.; Courville, A., *Deep Learning*, MIT Press, Cambridge (MA) 2016, p. 164-325; for adaptive learning see: Gama *et al.*, *op. cit.* note 14, p. 3-4.

¹⁸ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17 p. 164-325; Sculley, D. *et al.*, *op. cit.* note 16, p. 2506; Zhang *et al.*, *op. cit.* note 13, p. 1343.

¹⁹ Article 9 AI Act.

²⁰ Article 15(4) AI Act.

²¹ Article 43(3) AI Act.

By contrast, the MDR is primarily designed to ensure that only safe and effective medical devices are placed on the market.²² Its risk focus is centred on patient safety,²³ side effects,²⁴ risk-benefit considerations²⁵ and clinical efficacy.²⁶ While these elements are fundamental to product safety law, it remains questionable whether the MDR adequately captures the technological complexity and dynamic behaviour of continuously learning deep-learning modules.

Effective compliance with the AI Act requires careful consideration of the challenges posed by feedback loops²⁷ and continuous learning,²⁸ because these characteristics may lead to changes in predictive behaviour over time.²⁹ Despite several recitals addressing system modification, it remains unclear when a "continuous learning system" within the meaning of the AI Act must be regarded as having undergone a "substantial modification." Recital 128 AI Act provides only a general framework and does not offer conclusive criteria. As a result, the practical interpretation of "substantial modification" requires further legal clarification, particularly in the context of genetic diagnostics. This includes the question of whether retraining on new datasets necessitates a renewed conformity assessment and how such an obligation is to be operationalised in practice. Under Article 3(20) AI Act, a conformity assessment is a procedure designed to demonstrate whether a high-risk AI system complies with the requirements laid down in Title III, Section 2. With regard to high-risk AI systems, Article 43 AI Act establishes the applicable conformity assessment framework. The AI Act further provides for a presumption of conformity where systems comply with harmonised standards whose references have been published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012.³⁰ This raises a central question: whether the conformity assessment procedures under the MDR provide an equivalent and sufficiently comprehensive basis for such a presumption in the case of continuously learning genetic diagnostic systems. A core difficulty in applying the AI Act to genetic diagnostic systems lies in the adaptive nature of deep-learning algorithms, which may evolve

²² Recital 1, 2 MDR; *European Commission*, Commission Notice – The 'Blue Guide' on the implementation of EU product rules 2022, OJ C 247, 29.6.2022, 5, 12.

²³ Article 59, 80, 87, 89 MDR.

²⁴ Recital 8 MDR.

²⁵ Recital 81 MDR.

²⁶ For example, the general obligations of manufacturers in Article 10(9) in conjunction with Annex IX, Chapter I MDR.

²⁷ Sculley, D. *et al.*, *op. cit.* note 16, p. 2506.

²⁸ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325.

²⁹ *Ibid*; for adaptive learning see: Gama *et al.*, *op. cit.* note 14, p. 3-4.

³⁰ Feiler, L.; Forgó, N., Kommentar KI-VO, EU-Verordnung über künstliche Intelligenz, Verlag Österreich, Vienna 2024, p. 6.

over time.³¹ At the same time, Article 43(4), second sentence, clarifies that changes already taken into account in the original conformity assessment do not constitute significant changes. Thus, changes that occur within a previously defined and assessed framework do not constitute a "substantial modification" within the meaning of Article 43(4) AI Act and, accordingly, do not trigger a renewed conformity assessment.

However, in the context of genetic analysis, it remains uncertain what precisely constitutes a "substantial modification,"³² particularly where models are regularly retrained.³³ A deep-learning system performing genetic analyses may access new data post-deployment and detect correlations not covered by the initial conformity assessment. Such evolving behaviour may generate unreliable outputs, including erroneous diagnoses or risk predictions,³⁴ with potentially far-reaching consequences for patients and, indirectly, for biological relatives.

Finally, the concurrent application of the AI Act, MDR, and GDPR seeks to harmonise obligations for AI-based medical software.³⁵ Yet this regulatory layering also creates the risk of fragmentation, overregulation, and potential gaps in protection. Without a coherent doctrinal analysis of the interaction between these frameworks, there is a risk of both unnecessary regulatory burden³⁶ and insufficient safeguards for affected individuals. This is particularly relevant in the field of genetic diagnostics, where technical performance, clinical reliability, data protection, fundamental rights protection, and the interests of biological relatives are closely interlinked and cannot be assessed in isolation.

1.1. Methodology

This article adopts a doctrinal legal methodology. It undertakes a systematic and teleological interpretation of the AI Act and the Medical Device Regulation, with

³¹ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; for adaptive learning see: Gama *et al.*, *op. cit.* note 14, p. 3-4.

³² Medical Device Coordination Group (MDCG), *MDCG 2020-3 Rev.1 – Guidance on significant changes regarding the transitional provision under Article 120 MDR*, 2023, p. 3-5, https://health.ec.europa.eu/document/download/5fb74e56-fd4c-4dae-9d24-78149edfe56b_en?filename=md_mdcg_2020_3_rev1_en.pdf, accessed 21 February 2026. While the MDCG guidance is non-binding and drafted for Article 120 MDR devices; it is cited here solely as evidence of the regulator's event-based understanding of 'significant change' in practice.

³³ Zhang *et al.*, *op. cit.* note 13, p. 1336-1345.

³⁴ Zhang *et al.*, *op. cit.* note 13, p. 1343-1344; Wang, X. *et al.*, *op. cit.* note 13, p. 796–803.

³⁵ Recitals 8-10, 27, Article 43 AI Act.

³⁶ Herbst, T., *op. cit.* note 3, p. 246.

particular focus on their conformity assessment architectures and underlying regulatory assumptions. The analysis is based on the consolidated versions of Regulation (EU) 2024/1689 and Regulation (EU) 2017/745 as retrieved from EUR-Lex and the Official Journal of the European Union. Secondary literature was identified and reviewed through legal and interdisciplinary databases, including LexisNexis, Rechtsdatenbank Manz (hereinafter: RDB), and Beck-Online. The study further draws on guidance documents issued by the European Commission and the Medical Device Coordination Group (hereinafter: MDCG). Relevant interdisciplinary scholarship from medical and technical journals was reviewed where necessary to contextualise the regulatory analysis.

1.2. Structure of the article

Section 2 sets out the Annex I logic of the AI Act and explains how Article 43(3) links MDR conformity assessment to the AI Act's high-risk framework. Section 3 analyses MDR classification under Annex VIII, with particular focus on Rule 11 and its stability-oriented assumptions. Section 4 examines the ex ante structure of MDR conformity assessment under Annexes IX–XI, highlighting the implications for continuously learning genetic diagnostic software. Section 5 concludes by assessing the limits of functional equivalence underlying the presumption of conformity in this domain.

2. AI ACT ANNEX I LOGIC AND THE PRESUMPTION OF CONFORMITY

It is widely recognised in the literature that a deep-learning model used for disease diagnosis, prediction, or prognosis constitutes stand-alone software and is therefore subject to the MDR in addition to the AI Act.³⁷ Accordingly, a deep-learning model performing genetic analysis qualifies as a medical device within the meaning of Article 2(1) MDR and thus as a high-risk AI system pursuant to Article 6(1) AI Act. Continuous-learning genetic diagnostic systems therefore fall

³⁷ Königshofer, W., *op. cit.* note 2, para. 23; European Commission, *Medical devices: Guidance document – Qualification and Classification of stand-alone software (MEDDEV 2.1/6)*, July 2016, p. 9 *et seq.*, <https://ec.europa.eu/docsroom/documents/17921>, accessed 21 February 2026. This document is based on Directive 93/42/EEC; Annex II of the Council Resolution of 7 May 1985 on a new approach to technical harmonisation and standardisation (85/C 136/01), OJ C 1985/136, 1.; Schneeberger, D., *op. cit.* note 2, p. 5 *et seq.*

within Annex I, Section A AI Act³⁸ and are subject to the obligations applicable to high-risk AI systems, including requirements relating to risk management, bias mitigation, transparency, and conformity assessment.³⁹

In this regulatory constellation, the AI Act establishes a presumption of conformity for systems that comply with harmonised standards or parts thereof, provided that the references to those standards have been published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012.⁴⁰ Recital 46 AI Act confirms this classification by explicitly referring to the MDR as a Union harmonisation instrument. This confirms a sector-specific regulatory approach for high-risk AI systems listed in Annex I.⁴¹ Consequently, where an AI system falls within the scope of the MDR, it benefits from a rebuttable presumption of conformity with the corresponding requirements of the AI Act, in particular Articles 8 to 15.⁴² Subsumption under a harmonisation act such as the MDR entails that conformity must be demonstrated prior to placing the system on the market, in order to verify compliance with the applicable substantive requirements of that sectoral legislation.⁴³ In particular, Article 40 (1) AI Act—referring to conformity “to the extent that those standards cover those requirements or obligations”—underscores the need for individualised analysis and evaluation.

Chapter III, Section 2, Article 8(1) AI Act provides that the requirements set out in that section must be fulfilled, taking into account both the intended purpose and the state of the art in relation to AI. Article 8(2) further clarifies that providers of high-risk AI systems listed in Annex I, Section A bear responsibility for full compliance with all applicable requirements. Although formulated concisely, this provision establishes far-reaching obligations. The AI Act therefore applies in parallel to sector-specific legislation such as the MDR and complements, rather than replaces, the latter.⁴⁴ However, a separate AI Act risk management system is not required where the MDR already provides an equivalent framework, in which

³⁸ Feiler, L.; Forgó, N., *op. cit.* note 30, p. 11-12.

³⁹ Article 9 of the AI Act requires the implementation of a risk management system; in addition, a regular conformity assessment and associated monitoring as defined in Article 43 of the AI Act is required.

⁴⁰ Feiler, L.; Forgó, N., *op. cit.* note 30, p. 6.6.

⁴¹ Forgó, N.; Prainsack, B., New AI regulation in the EU seeks to reduce risk without assessing public benefit, *Nature Medicine*, 30(5), 2024, p. 1235, doi: 10.1038/s41591-024-02874-2; Feiler, L.; Forgó, N., *op. cit.* note 30, p. 14-15.

⁴² Article 40 AI Act, Feiler, L.; Forgó, N., *op. cit.* note 30, p. 10.

⁴³ Feiler, L.; Forgó, N., *op. cit.* note 30, p. 10.

⁴⁴ Recital 64 AI Act; Feiler, L.; Forgó, N., *op. cit.* note 30, p. 11-12.

case compliance under the MDR may give rise to a presumption of conformity under the AI Act.⁴⁵

Pursuant to Article 16(f) in conjunction with Article 43 AI Act, providers must carry out a conformity assessment prior to placing a high-risk AI system on the market or putting it into service. While Article 42 AI Act establishes a presumption of conformity for compliance with harmonised standards, this presumption does not automatically extend to the conformity assessment procedure itself. Article 43(3) AI Act addresses this interaction by providing that, for high-risk AI systems covered by Union harmonisation acts listed in Annex I, Section A – including the MDR – the conformity assessment procedures under the relevant sectoral legislation apply in lieu of the stand-alone AI Act procedure. However, the substantive requirements of Chapter III, Section 2 AI Act continue to apply. As established above, a continuous deep-learning model used for genetic diagnosis qualifies as stand-alone software and thus as a medical device under Article 2(1) MDR.⁴⁶ Article 2(4) MDR further clarifies that software constitutes an active medical device. Consequently, pursuant to Article 43(3) AI Act, such systems must undergo the conformity assessment procedure established under the MDR as the applicable sectoral harmonisation act.

The presumption of conformity rests on the assumption that the relevant harmonised standards and sectoral conformity procedures sufficiently cover the substantive requirements imposed by the AI Act. This assumption warrants critical scrutiny. The MDR was adopted prior to the emergence of continuously learning AI systems as a central regulatory object and was not specifically designed to address the technical and epistemic characteristics of adaptive deep-learning architectures.⁴⁷ It therefore remains questionable whether conformity assessment

⁴⁵ Recital 22 MDR, which emphasises the importance of harmonised standards for medical devices.

⁴⁶ Article 2(1) first sentence *Regulation (EU) 2017/745* of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 2017/117; Königshofer, W., *op. cit.* note 2, para. 23; European Commission, *Medical devices: Guidance document – Qualification and Classification of stand alone software (MEDDEV 2.1/6)*, July 2016, p. 9 *et seq.*, <https://ec.europa.eu/docsroom/documents/17921>, accessed 21 February 2026. This document is based on Directive 93/42/EEC; Annex II of the Council Resolution of 7 May 1985 on a new approach to technical harmonisation and standardisation (85/C 136/01), OJ C 1985/136, 1; Schneeberger, D., *op. cit.* note 2, p. 5 *et seq.*

⁴⁷ U.S. Food and Drug Administration (FDA), Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD): Discussion Paper and Request for Feedback, 2019, <https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial->

under the MDR adequately captures the technical complexities and adaptive characteristics of continuously learning high-risk AI systems. Although Article 43(3) AI Act seeks to integrate the requirements of Chapter III, Section 2 into the sectoral conformity assessment, the structural design of the MDR may not be fully equivalent for systems characterised by ongoing behavioural evolution. Accordingly, this structural tension forms the starting point for the subsequent analysis.

3. MDR CLASSIFICATION: RULE 11 AND INSTABILITY FOR CONTINUOUS LEARNING

As set out in Chapter V MDR, the conformity assessment procedure serves to demonstrate whether a device complies with the requirements laid down in the Regulation.⁴⁸ Before determining the applicable conformity assessment route, a deep-learning system conducting genetic analysis must first be qualified and classified under the MDR. Pursuant to Article 51(1) MDR, medical devices are divided into classes I, IIa, IIb and III, taking into account their intended purpose and the inherent risks associated with their use. The determination of the intended purpose therefore operates as a decisive gatekeeper for the subsequent classification exercise. However, the classification of continuously learning deep-learning systems under Annex VIII MDR raises significant conceptual and practical challenges.

3.1 Duration of Use and the Static Product Paradigm

At an early stage of the classification exercise, Chapter I, Section 1 of Annex VIII MDR introduces a distinction between transient, short-term and long-term use. Duration of use is defined according to whether a device is intended for continuous use of less than 60 minutes, between 60 minutes and 30 days, or for long-term use exceeding 30 days. In the context of a continuously learning deep-learning model, the meaning of "duration of use" becomes ambiguous, because it is unclear whether this notion captures only the moment at which the system performs a specific genetic analysis, or whether it extends to the model's full lifecycle once deployed and continuously updated. Continuous-learning systems do not exhibit clearly bounded "use phases" in the manner presupposed by the MDR. Instead,

Intelligence-and-Machine-Learning-Discussion-Paper.pdf, p. 1, accessed 21 February 2026.

⁴⁸ Recital 4 MDR.

they may remain operational indefinitely, while their internal parameters evolve over time.⁴⁹ This ambiguity reveals an underlying structural assumption of the MDR: First, the Regulation is predicated on the notion of a fixed, self-contained product with a definable beginning and end of its lifecycle. Second, it suggests that the classification framework was primarily designed for stable and static devices, rather than for continuously evolving, data-driven systems whose performance characteristics may change after market placement.

Annex VIII Section 3.6(a) further clarifies that "continuous use" refers to the entire duration of use of the same device, irrespective of temporary interruptions (for example, for cleaning or disinfection). Such examples reflect a paradigm tailored to tangible, physical devices. By contrast, updating, monitoring, or retraining a deep-learning system constitutes a fundamentally different process from cleaning or temporarily removing a physical device. Continuous-learning architectures therefore strain the conceptual categories embedded in the MDR classification framework.

Additional complexity arises from Implementing Rule 3.5(b), which addresses accumulated use where a device is intended to be replaced immediately by another device of the same type. In the context of continuously retrained models, each updated algorithmic version could arguably be interpreted as a functional replacement of the previous iteration.⁵⁰ This raises a doctrinally sensitive question: what constitutes the relevant "device" for classification purposes—the initial approved model architecture, each retrained version, or the evolving system as a whole? The temporal cycle of continuous learning is therefore difficult to reconcile with the static product-based logic underlying Annex VIII.

Moving further, Rule 11 of Annex VIII MDR has been identified in both guidance and literature as the central classification rule for software performing diagnostic or therapeutic functions.⁵¹ Under Rule 11, software intended to provide

⁴⁹ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; Sculley, D. *et al.*, *op. cit.* note 16, p. 2506; for adaptive learning see: Gama *et al.*, *op. cit.* note 14, p. 3-4.

⁵⁰ Medical Device Coordination Group (MDCG), *MDCG 2020-3 Rev.1 – Guidance on significant changes regarding the transitional provision under Article 120 MDR*, 2023, p. 12, https://health.ec.europa.eu/document/download/5fb74e56-fd4c-4dae-9d24-78149edfe56b_en?filename=md_mdcg_2020_3_rev1_en.pdf, accessed 21 February 2026.

⁵¹ Königshofer, W., *op. cit.* note 2, para. 23; European Commission, *Medical devices: Guidance document – Qualification and Classification of stand alone software (MEDDEV 2.1/6)*, July 2016, p. 9 *et seq.*, <https://ec.europa.eu/docsroom/documents/17921>, accessed 21 February 2026. This document is based on Directive 93/42/EEC; Annex II of the Council Resolution of 7 May 1985 on a new approach to technical harmonisation and standardisation (85/C 136/01), OJ C 1985/136, 1; Schneeberger, D., *op. cit.* note 2, p. 5 *et seq.*

information used to make decisions for diagnostic or therapeutic purposes is classified as class IIa. However, Rule 11 introduces an escalation mechanism: where decisions supported by the software may cause death or irreversible deterioration of a person's state of health, the software is classified as class III. Where such decisions may cause serious deterioration of health or require surgical intervention, the software is classified as class IIb. This differentiation is particularly challenging in the context of AI-based systems, as it raises the question of where the relevant threshold is to be drawn, especially given the distinction between foreseen and unforeseen risks.

In the field of genetic analysis, incorrect assessments—especially if combined with ineffective human oversight—may lead to undetected hereditary diseases, misidentified diagnostic risks, or inappropriate treatment decisions.⁵² Such failures may have severe consequences not only for the patient but also, indirectly, for biological relatives. In these scenarios, it becomes difficult to determine whether the system should be classified as class IIb or class III, and which legal criteria should govern this determination. Rule 11 also provides that software intended to monitor physiological processes is classified as class IIa, except where monitoring of vital physiological parameters may result in immediate danger to the patient, in which case classification shifts to class IIb. All other software falls into class I. This residual category is particularly problematic in the AI context. A deep-learning system may escape higher classification if neither a clear causal link nor a sufficiently concrete likelihood of severe harm can be established. This outcome is reinforced by the MDR's structural assumption of effective human oversight. The classification logic presumes that clinicians retain ultimate decision-making authority and can identify and correct erroneous outputs. In the context of opaque ("black-box") models and continuous learning,⁵³ however, this assumption may function as a normative fiction. If oversight is limited in practice, the risk profile of the system may exceed what is reflected in its formal classification.

An intermediate approach may be to classify the deep-learning module as class Iia, where the likelihood of death, irreversible deterioration⁵⁴, or serious deterioration of a person's state of health⁵⁵ cannot be sufficiently established at the time of assessment. Yet this solution forces a continuously evolving system into a fixed regulatory category. This tension becomes particularly evident when considering the technical dynamics of adaptive models. Continuous-learning

⁵² Zhang *et al.*, *op. cit.* note 13, p. 1343-1344; Wang, X. *et al.*, *op. cit.* note 13, p. 796–803.

⁵³ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; for adaptive learning see: Gama *et al.*, *op. cit.* note 14, p. 3-4, p. 30.

⁵⁴ Annex VIII, Chapter III, Rule 11, Sentence 1 MDR.

⁵⁵ Annex VIII, Chapter III, Rule 11, Sentence 2 MDR.

systems may change their performance characteristics over time. As new data are incorporated and internal parameters are updated, the system's predictive accuracy, error patterns, and clinical impact may shift.⁵⁶ Consequently, a model initially classified as class IIa could, in practice, begin to support decisions that entail a higher risk profile, potentially falling within the scope of class IIb or even class III.

Rule 11 provides no explicit mechanism to accommodate such dynamic risk evolution. Classification is performed *ex ante*, based on the intended purpose⁵⁷ and foreseeable risks⁵⁸ at the time of conformity assessment.⁵⁹ It does not contain a structured framework for reassessing classification where risk profiles evolve due to adaptive learning. Consequently, classification under Rule 11 is conducted on a case-by-case basis, often relying on interpretative guidance and the assessment of notified bodies, without clearly defined criteria for continuous-learning systems. The wording "may cause"⁶⁰ reinforces this tension. It presupposes a relatively stable and foreseeable risk scenario, whereas continuously learning systems operate within dynamic and probabilistic environments.⁶¹ The combination of *ex ante* classification logic and evolving model behaviour creates a structural mismatch between regulatory design and technological reality.

In sum, the classification regime under Annex VIII—particularly Rule 11—reflects a stability-oriented regulatory paradigm. When applied to continuously learning deep-learning systems in genetic diagnostics, this paradigm produces instability, uncertainty, and potential under- or over-classification. The static classification logic of the MDR therefore, sits uneasily with adaptive AI technologies whose risk profiles may evolve after market placement.

4. MDR CONFORMITY ASSESSMENT IS STRUCTURALLY EX ANTE

The analysis above demonstrates that the foundation for conformity assessment procedures and routes provided under Article 52 MDR and Annexes IX to XI are inherently *ex ante* in nature. Their design is explicitly oriented toward the period

⁵⁶ Gama *et al.*, *op. cit.* note 14, p. 3-4; Zhang *et al.*, *op. cit.* note 13, p. 1343-1345.

⁵⁷ Article 2(12) MDR; Annex VIII, Chapter II, Section 3.1 MDR

⁵⁸ Annex I, Chapter I, Section 8 MDR.

⁵⁹ Annex IX-XI MDR.

⁶⁰ Annex VIII, Chapter III, Rule 11, Sentence 1 MDR.

⁶¹ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; for feedback loops: Sculley, D. *et al.*, *op. cit.* note 16, p. 2506.

prior to placing the device on the market or putting it into service. This temporal orientation reflects an implicit structural assumption: that the device assessed during conformity evaluation will remain materially unchanged thereafter.

This assumption entails that the medical device is characterised by a defined technical configuration, a fixed and declared intended purpose, and a stable risk profile.⁶² It further presupposes that no additional functionalities, risk dynamics, or inferential capacities emerge beyond those foreseeable at the time of assessment. In particular, it assumes that system behaviour will remain within the scope of what was documented, tested, and certified, thereby excluding the dynamic effects of continuous learning, feedback loops⁶³ or post-deployment adaptation. Feedback loops may alter the distribution of training data, resulting in parameter updates and shifts in decision boundaries,⁶⁴ which in turn may lead to different predictive outputs over time. In genetic diagnostic contexts, such shifts may surface previously non-salient probabilistic associations, including risk correlations that were not reflected in the originally assessed configuration and that may have implications for biological relatives.

By contrast, the technical architecture of continuously learning deep-learning systems departs fundamentally from this stability paradigm. Not all AI- and machine-learning-based software medical devices are "locked".⁶⁵ In this context, "locked" describes an algorithm that provides the same result each time the same input is provided, whereas a continuous learning algorithm adapts its behaviour using a specified learning process. Whereas locked algorithms produce identical outputs for identical inputs,⁶⁶ continuously learning systems are capable of modifying internal parameters during operation. Through retraining, dataset updates, or parameter optimisation, such systems may alter their performance characteristics over time.⁶⁷ Their defining feature is precisely the capacity for

⁶² See, e.g., Art 2(12) MDR.

⁶³ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; for feedback loops: Sculley *et al.*, *op. cit.* note 16, p. 2506.

⁶⁴ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; Sculley, D. *et al.*, *op. cit.* note 16, p. 2506.

⁶⁵ U.S. Food and Drug Administration (FDA), Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD): Discussion Paper and Request for Feedback, 2019, p. 3, <https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf>, accessed 21 February 2026.

⁶⁶ *Ibid.*, p. 3.

⁶⁷ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; for feedback loops: Sculley, D. *et al.*, *op. cit.* note 16, p. 2506; Zhang *et al.*, *op. cit.* note 13, p. 1343-1345.

behavioural adaptation based on real-world use.⁶⁸ It can be argued that regulatory frameworks originally developed for physical or functionally stable devices did not anticipate such ongoing model evolution.⁶⁹ The core tension therefore, lies in a conformity assessment that evaluates a specific historical model state, while the operational system continues to evolve after certification. Conformity assessment is temporally anchored; system behaviour is temporally dynamic.

The MDR was not originally conceived with continuously learning software as a central regulatory object.⁷⁰ Although the Regulation formally encompasses software, its structural architecture reflects a product-based paradigm centred on identifiable configurations and foreseeable risks. It remains, therefore, ambiguous whether the MDR's obligations are sufficiently tailored to address continuously adaptive deep-learning systems conducting genetic analysis, particularly where changes in data environments and post-deployment updating can alter outputs, which may facilitate secondary (relational) inferences concerning biological relatives.⁷¹ Having identified the *ex ante* character of conformity assessment under the MDR, it becomes necessary to examine the substantive mechanisms through which conformity is verified. In functional terms, conformity assessment under the MDR rests on three core components: (1) auditing the quality management system (hereinafter: QMS), (2) assessing technical documentation, and (3)

⁶⁸ U.S. Food and Drug Administration (FDA), Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD): Discussion Paper and Request for Feedback, 2019, p. 1, 3-4, 7, <https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf>, accessed 21 February 2026.

⁶⁹ Ludvigsen, K.R.; Nagaraja, S.; Daly, A., The Intention; Requirements for Software as a Medical Device in EU Law, SSRN Paper, 2021, p. 1; see further: U.S. Food and Drug Administration (FDA), Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD): Discussion Paper and Request for Feedback, 2019, <https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf>, p. 2, accessed 21 February 2026.

⁷⁰ Ludvigsen, K.R.; Nagaraja, S.; Daly, A., *op. cit.* note 69, p. 1; see further: U.S. Food and Drug Administration (FDA), Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD): Discussion Paper and Request for Feedback, 2019, p. 2, <https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf>, accessed 21 February 2026.

⁷¹ Erlich, Y.; Narayanan, A., Routes for Breaching and Protecting Genetic Privacy, *Nature Reviews Genetics*, 15, 2014, p. 417. doi:10.1038/nrg3723; on system evolution and feedback loops see: Sculley, D. *et al.*, *op. cit.* note 16, p. 2506; see also: Spiliopoulou A. *et al.*, Genomic Prediction of Complex Human Traits: Relatedness, Trait Architecture and Predictive Meta-Models, *Human Molecular Genetics*, 24(14), 2015, p. 4168-4169, doi:10.1093/hmg/ddv145.

performing verification and validation testing.⁷² The QMS framework requires documented procedures and predefined control mechanisms, with technical documentation capturing the device's characteristics at a specific point in time. Verification and validation testing assess the performance of a defined system configuration before market placement. This assumes that the tested and documented configuration remains representative of the device's ongoing operational behaviour. Consequently, the conformity assessment regime assumes stability of device identity over time.

For continuously learning systems, however, this assumption becomes fragile. As internal parameters evolve and performance characteristics shift, the relationship between the originally certified configuration and the deployed system may weaken. A deep-learning module initially assessed under a particular risk classification may, over time, exhibit altered error patterns or enhanced inferential capacities that were neither fully foreseeable nor fully representable at the time of assessment. This structural tension is further amplified by the technical complexity of genetic analysis systems. In the context of genetic analysis, deep-learning systems may facilitate indirect or relational inferences concerning biological relatives.⁷³ Where such systems undergo retraining or adaptation, the scope or precision of such inferences may shift over time⁷⁴ or enable emergent correlations not explicitly programmed.⁷⁵ As a result, manufacturers may seek to limit the scope of outputs through predefined design constraints or specification of intended use.⁷⁶ However, such modifications may influence performance metrics and error distributions, thereby affecting the system's effective risk profile.⁷⁷ These dynamics sit uneasily with a conformity logic that relies on *ex ante* assumptions regarding device behaviour and foreseeable risks, while largely excluding systematic reassessment of evolving characteristics during deployment. This results in a temporal asymmetry; while conformity assessment is completed at a fixed moment, the risk evolution may continue throughout the lifecycle of the device. In this respect, the *ex ante* evidentiary structure of the MDR does not result

⁷² Stange, A.F.; Julian, E., *Conformity Assessment of Medical Devices*, *Journal of Market Access & Health Policy*, 14(1):4, 2026, p. 2. doi:10.3390/jmahp14010004.

⁷³ Erlich, Y.; Narayanan, A., *op. cit.* note 71, p. 417; on system evolution and feedback loops see: Sculley, D. *et al.*, *op. cit.* note 16, p. 2506; see also: Spiliopoulou A. *et al.*, *op. cit.* note 71, p. 4168-4169.

⁷⁴ Erlich, Y.; Narayanan, A., *op. cit.* note 71, p. 417; on system evolution and feedback loops see: Sculley, D. *et al.*, *op. cit.* note 16, p. 2506; see also: Spiliopoulou A. *et al.*, *op. cit.* note 71, p. 4168-4169.

⁷⁵ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; for feedback loops: Sculley, D. *et al.*, *op. cit.* note 16, p. 2506; Zhang *et al.*, *op. cit.* note 13, p. 1343-1345.

⁷⁶ See: Article 2(12), Annex II MDR.

⁷⁷ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; for feedback loops: Sculley, D. *et al.*, *op. cit.* note 16, p. 2506; Zhang *et al.*, *op. cit.* note 13, p. 1343-1345.

in an enforcement challenge; rather, it reveals a design limitation when applied to continuously evolving AI systems. Consequently, even with full formal compliance, the conformity assessment may fail to capture behavioural developments that occur post-certification. In summary, the structural architecture of the MDR presupposes stability, whereas continuous-learning systems are structured by evolution.

4.1 Annex IX MDR: Quality Management System and Controlled Change

Annex IX MDR establishes a conformity assessment procedure centred on a quality management system combined with technical documentation, thereby grounding conformity assessment in a predominantly process-oriented framework designed to preserve effectiveness throughout the device's lifecycle.⁷⁸ Annex IX constitutes the standard conformity assessment route for devices classified as class IIa, IIb, and III. Chapter I, Section 2 specifies the QMS requirements, complemented by the technical documentation obligations in Chapter II. The QMS framework itself is structurally divided into an *ex ante* component (Section 2) and a post-market surveillance and monitoring component (Section 3).

Proportionate to the applicable risk class and the nature of the device,⁷⁹ this architecture reflects a regulatory model premised on predefined system controls and documented procedures. It assumes that compliance can be secured through organisational safeguards, documented responsibilities, traceability mechanisms, and monitored corrective processes.⁸⁰ The focus lies on process integrity and control structures rather than on continuous substantive reassessment of evolving outputs or adaptive learning dynamics. Although Annex IX incorporates post-market surveillance, its structure channels post-certification changes primarily through documentation, monitoring, and — where necessary — renewed conformity assessment. It does not establish a mechanism for ongoing substantive re-evaluation of device behaviour as such. The regulatory emphasis remains procedural rather than behavioural.

The MDR recognises that medical devices may undergo design modifications after conformity assessment, compliance may be preserved where the manufacturer operates a QMS capable of managing such modifications within appropriate frames and ensuring continued conformity with the applicable procedure.⁸¹ In this

⁷⁸ Stange, A.F.; Julian, E., *op. cit.* note 72, p. 3.

⁷⁹ Recital 32 MDR.

⁸⁰ Annex IX, Chapter I, Section 2.1 and 2.2 MDR.

⁸¹ Article 10(9) MDR.

context, software devices may incorporate recalibration or reconfiguration functionalities, provided that such modifications occur within predefined boundaries that were covered by the initial conformity assessment.⁸² The QMS therefore operates as a governance structure for controlled change, not as a substitute for substantive reassessment. Crucially, these modifications must remain within the originally declared intended purpose prior to market placement,⁸³ which entails manufacturers are prohibited from recommending uses deviating from the intended purpose underlying the conformity assessment.⁸⁴ Furthermore, planned substantial changes must be communicated to the notified body.⁸⁵ The conformity architecture thus presupposes that relevant modifications are identifiable, intentional, and assessable within a controlled change framework.

This logic aligns comfortably with "locked" AI systems, which generate identical outputs for identical inputs.⁸⁶ It also accommodates adaptive systems operating within predefined change envelopes covered by the original conformity assessment.⁸⁷ Therefore, it presupposes that adaptive capacity is ex ante limited, foreseeable, and governable through predefined tolerance ranges.

However, deep-learning architectures may, by virtue of their technological design, evolve beyond such predefined boundaries. As a consequence of their adaptive capabilities, these systems may exhibit behaviour that exceeds the limits initially assessed and thereby fall outside the scope of the original conformity assessment. Accordingly, deep-learning modules challenge the regulatory assumptions underlying the MDR, which are premised on behavioural stability and ex ante foreseeable developments. In this respect, Annex IX does not provide a dedicated mechanism to accommodate continuous behavioural evolution within the same conformity framework. Its regulatory logic permits adaptability only insofar as it remains ex ante bounded and controllable through predetermined organisational

⁸² Predefined modification during runtime refers to adjustments, optimisation, or recalibration of a medical software device within these predefined boundaries, in relation to an individual patient or a specific healthcare environment. See: COCIR – European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry, *Artificial intelligence in EU medical device legislation*, 2021, p. 10, https://cocir.org/uploads/2021/10/COCIR_AI_in_EU_Medical_Device_Legislation_2021.pdf, accessed 21 February 2026.

⁸³ *Ibid.*, p. 9.

⁸⁴ Article 7(d) MDR.

⁸⁵ Annex IX, Chapter I, Section 2.4 MDR.

⁸⁶ COCIR – European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry, *Artificial intelligence in EU medical device legislation*, 2021, p. 10, https://cocir.org/uploads/2021/10/COCIR_AI_in_EU_Medical_Device_Legislation_2021.pdf, accessed 21 February 2026.

⁸⁷ *Ibid.*, p. 12.

safeguards.⁸⁸ Once adaptive behaviour extends beyond those predefined limits, the architecture reverts to the dichotomy of either triggering a new conformity assessment or operating outside the assessed scope.

This reveals the structural tension underlying Annex IX: procedurally, it is comprehensive; substantively, it presupposes behavioural stability. The framework offers extensive documentation, monitoring, and quality control mechanisms. Yet these mechanisms remain anchored in the assumption that relevant behavioural change is either planned or foreseeable within predefined boundaries.

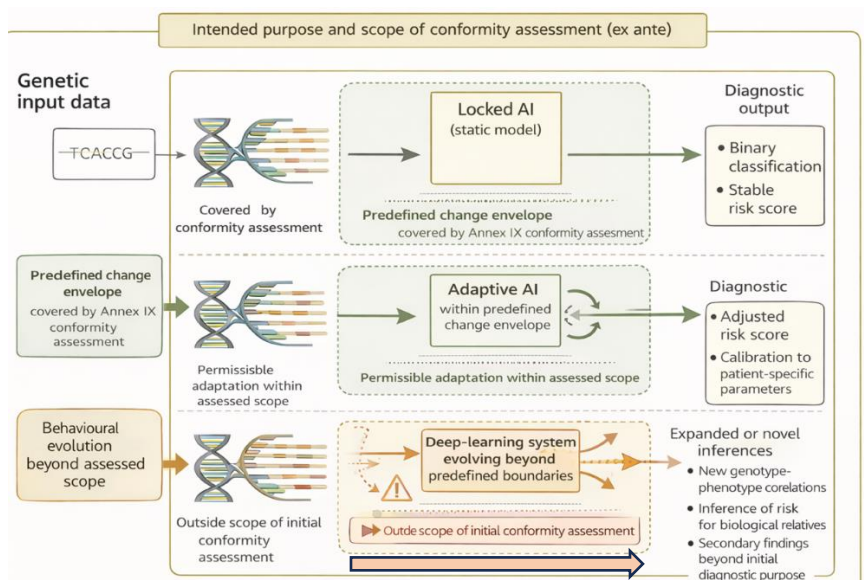


Figure 1: Input-output-based illustration of algorithmic change scenarios in AI-based genetic diagnostic systems under Annex IX MDR. The figure contrasts locked AI, adaptive AI operating within predefined change boundaries covered by conformity assessment, and deep-learning systems evolving beyond the assessed scope, highlighting the regulatory implications of behavioural evolution at output level.⁸⁹

⁸⁸ COCIR – European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry, *Artificial intelligence in EU medical device legislation*, 2021, p. 12, https://cocir.org/uploads/2021/10/COCIR_AI_in_EU_Medical_Device_Legislation_2021.pdf, accessed 21 February 2026.

⁸⁹ The conceptual design of this figure was developed by the author with the assistance of an AI-based language model (ChatGPT) and subsequently refined for academic use. The substantive content, legal analysis, and interpretation remain the sole responsibility of the author.

For continuously learning systems in genetic diagnostics, where model behaviour may evolve in response to real-world data and generate new inferential patterns, this assumption becomes increasingly fragile. The regulatory completeness of Annex IX at the procedural level thus coexists with a substantive blind spot at the behavioural level.

4.2. Technical documentation and testing under the MDR

Manufacturers of medical devices are required to establish technical documentation for the purpose of demonstrating conformity with the requirements of the MDR. Annex II MDR sets out the substantive requirements for such documentation and primarily operates as an *ex ante* regulatory instrument, whereas Annex III complements this framework by governing post-market surveillance documentation.⁹⁰

The structure of technical documentation under Annex II reflects its function as the substantive evidentiary foundation of conformity assessment. Conformity is verified through a documentation-based assessment of the device's technical characteristics, performance claims, and risk profile at the time of submission. By its very nature, this assessment captures the device at a defined point in time. Technical documentation, therefore reflects a regulatory snapshot rather than the ongoing behavioural development of a system during operation.

For continuously learning deep-learning systems used in genetic diagnostics, this snapshot logic becomes problematic. Where system behaviour evolves through retraining, feedback loops, or changing data environments,⁹¹ a documentation-based assessment may not fully represent the device's future operational characteristics. The evidentiary model presupposes temporal stability; adaptive architectures introduce temporal dynamism. Annex II further requires that technical documentation be presented in a "clear, organised, readily searchable and unambiguous manner" and accurately reflect the characteristics of the medical software device at the time of submission. Central to this documentation are the device description and specification, including the intended purpose and intended users.⁹² These elements function as fixed regulatory reference points and are defined *ex ante* by the manufacturer within the conformity assessment dossier.

⁹⁰ Article 10(4) MDR.

⁹¹ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; Zhang *et al.*, *op. cit.* note 13, p. 1343-1345; for feedback loops: Sculley, D. *et al.*, *op. cit.* note 16, p. 2506.

⁹² Annex II, Section 1.1(a) MDR.

This ex ante fixation becomes structurally fragile where feedback-driven updates⁹³ or evolving deployment conditions⁹⁴ alter model behaviour over time. In systems processing inherently relational genetic data, behavioural evolution may affect the scope of inferential outputs, potentially extending beyond the initially declared intended purpose and indirectly implicating biological relatives. Outputs may generate secondary inferences concerning biological relatives⁹⁵ and thereby expand the practical scope of the device's impact, even in the absence of formal modifications to the model architecture or algorithm.⁹⁶ The conformity assessment remains formally intact; yet the behavioural reach of the system may expand beyond what was initially documented. The result is not necessarily non-compliance, but rather a structural risk of regulatory incompleteness after submission of the technical documentation⁹⁷ While the conformity framework presupposes that the documented configuration remains representative of the deployed system, continuous learning challenges that presupposition.

The ex ante logic is further reinforced in Annex II, Point 6, which requires the inclusion of "results and critical analyses of all verifications and validation tests and/or studies undertaken to demonstrate conformity of the device with the requirements of the MDR." Verification and validation are conducted on a defined system configuration prior to market placement. In continuously learning systems, however, operational behaviour may evolve post-deployment through parameter updates or changing data distributions, even where the underlying architecture remains unchanged.⁹⁸

Testing and validation under the MDR therefore focus on the demonstrated performance of a particular model state, rather than on the adaptive trajectory of the system over time. The regulatory assumption underlying this framework is that the validated configuration remains sufficiently representative of the device's

⁹³ Sculley, D. *et al.*, *op. cit.* note 16, p. 2506.

⁹⁴ Zhang *et al.*, *op. cit.* note 13, p. 1343-1345.

⁹⁵ Erlich, Y.; Narayanan, A., *op. cit.* note 71, p. 417; Spiliopoulou A. *et al.*, *op. cit.* note 71, p. 4168-4169; on system evolution and feedback loops see: Sculley, D. *et al.*, *op. cit.* note 16, p. 2506.

⁹⁶ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; Zhang *et al.*, *op. cit.* note 13, p. 1343-1345; for feedback loops: Sculley, D. *et al.*, *op. cit.* note 16, p. 2506.

⁹⁷ Additionally, the feedback loops and model performance may improve unevenly among different sub-populations groups. For example, see: Zhang *et al.*, *op. cit.* note 13, p. 1331, 1342; Seyyed-Kalantari, L. *et al.*, CheXclusion: Fairness Gaps in Deep Chest X-Ray Classifiers, Pacific Symposium Biocomputing, 26, 2021, p. 232-243. However, this thesis does not focus on bias and ethical issues in this context, therefore it remains mentioned but not analysed in detail due to the limitation of the objective of the paper.

⁹⁸ Gama *et al.*, *op. cit.* note 14, p. 4.

future operational behaviour. However continuous-learning architectures render that assumption contestable.

In this respect, the conformity architecture of the MDR does not merely impose extensive documentation obligations; it embodies a specific epistemic model of regulatory control. That model is oriented toward identifiable, stable configurations capable of being documented, tested, and certified. Where system behaviour evolves beyond that configuration through ongoing learning processes, the correspondence between certified documentation and operational reality may progressively weaken.

4.3 Annex X MDR: Type Examination and Static Device Assumptions

Annex X establishes the EU type-examination procedure, under which a notified body assesses and certifies that a medical device complies with the applicable provisions of the MDR. In this procedure, the notified body examines the technical documentation, evaluates relevant lifecycle processes, and requires a representative sample of the envisaged device production. Conformity is established through the assessment of a representative specimen, which presupposes that the essential characteristics of the device — including its performance parameters — remain sufficiently stable over time. This reflects a type-examination logic that is structurally *ex ante*. The assessment framework under Annex X presupposes a medical device whose relevant characteristics are sufficiently stable at the time of market placement to allow certification on the basis of a defined set of technical parameters.⁹⁹ Conformity assessment is therefore conducted at a specific moment in time, with the implicit expectation that this evaluation remains representative of the device's subsequent performance.

In the context of continuously learning software systems, this expectation becomes fragile again, because behavioural parameters may evolve during deployment through retraining, dataset shifts, or internal parameter updates,¹⁰⁰ potentially altering performance characteristics after certification. Annex X does not expressly provide a mechanism to evaluate prospective behavioural evolution at the time of assessment. The notified body verifies conformity on the basis of documented and tested characteristics of the submitted configuration,¹⁰¹ rather

⁹⁹ Article 56, Annex II, Annex X Section 4 MDR.

¹⁰⁰ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; for feedback loops: Sculley, D. *et al.*, *op. cit.* note 16, p. 2506; Zhang *et al.*, *op. cit.* note 13, p. 1343-1345.

¹⁰¹ Article 52 MDR, Annex IX, Annex II MDR.

than on the basis of dynamically unfolding operational behaviour. As a result, a temporal asymmetry arises between the certification snapshot and the subsequent evolution of the system during real-world use. The rigidity of the type-examination model is further reinforced by Annex II, Section 5, which governs changes to the approved type. Manufacturers must inform the notified body of any planned change to the approved medical device or to its intended purpose and conditions of use.¹⁰² The emphasis on "planned" modifications reflects an assumption that relevant changes are identifiable, intentional, and temporally bounded. Continuously learning systems challenge this assumption, because adaptive behaviour may expand functional scope, alter inferential capacities, or modify performance characteristics without a discrete, intentionally planned intervention by the manufacturer. Where such evolution affects the intended purpose or conditions of use, renewed approval may be required. Continuous learning could therefore repeatedly trigger the obligation to conduct a new conformity assessment.

Annex X thus reinforces the stability-oriented paradigm underlying the MDR. Type-examination is designed for devices whose essential characteristics can be fixed, documented, and certified as a stable reference configuration. Consequently, continuously learning architectures destabilise the notion of a single identifiable "type", thereby exposing the structural limits of the type-examination model.

4.4 Annex XI MDR: Product Conformity Verification and Output-Oriented Control

Conformity assessment under Annex XI constitutes the third conformity assessment pathway available under Article 52 MDR. Annex XI operates as a verification mechanism and builds upon prior conformity assessment steps, particularly the European Union type-examination (hereinafter: EU type-examination) under Annex X.¹⁰³ In line with Annexes IX and X, Annex XI presupposes a previously defined and approved device type derived from the prior EU type-examination. Part A of Annex XI focuses on production quality assurance through the implementation and surveillance of an approved quality management system. Verification of such a system presupposes the continued implementation of an established compliance structure. It does not, however, entail an independent reassessment of evolving behavioural characteristics inherent in a continuously learning software device. The conformity logic remains anchored in the approved

¹⁰² Annex II, Section 5.1 MDR.

¹⁰³ Article 52 MDR; Annex XI, Section 1 MDR.

type and the manufacturer's obligation to ensure that production consistently corresponds to that certified configuration. The manufacturer's obligation to certify and declare conformity with the type described in the EU type-examination certificate presupposes a stable and identifiable device identity. This assumption becomes fragile where behavioural evolution occurs in a continuously learning module, as the operational system may progressively diverge from the originally approved type without a discrete, formally identifiable modification event. Part B establishes a product verification procedure requiring the examination of each manufactured device to ensure and declare its conformity with the type described in the EU type-examination certificate and with the applicable requirements of the MDR.¹⁰⁴ This examination-based model presupposes identifiable units characterised by defined parameters, stable testing conditions, and reproducible characteristics. In the context of physical devices, this unit-by-unit verification logic is conceptually coherent; in contrast, centrally deployed or cloud-based software architectures may involve ongoing model update cycles and continuously learning features at the level of neural network parameters.¹⁰⁵ Parameter adjustments, retraining processes, and evolving data distributions may lead to version modifications and shifting operational states over time.¹⁰⁶ Such evolution challenges the representativeness of the examined configuration and raises the question of which model state constitutes the relevant "device" for purposes of verification.

Continuous learning architectures are characterised by parameter updates and evolving model states across training and update cycles.¹⁰⁷ Consequently, continuously learning systems introduce evolving parameter states during operation. This creates a structural tension between the unit-by-unit verification logic embedded in Annex XI and the fluid, model-state-based nature of adaptive AI systems. Where the certified configuration is no longer identical to the deployed configuration, the conceptual basis of product verification — namely, conformity with a stable approved type — becomes increasingly difficult to maintain.

Annex XI therefore, does not depart from the stability-oriented paradigm underlying Annex X; rather, it reinforces it. Product verification and production quality assurance remain anchored in the assumption of a fixed and reproducible device identity. For continuously learning genetic diagnostic systems, this

¹⁰⁴ Annex XI, Part B, Section 11 MDR.

¹⁰⁵ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325; Sculley, D. *et al.*, *op. cit.* note 16, p. 2506; Zhang *et al.*, *op. cit.* note 13, p. 1343-1345.

¹⁰⁶ Sculley, D. *et al.*, *op. cit.* note 16, p. 2506; Zhang *et al.*, *op. cit.* note 13, p. 1333-1335.

¹⁰⁷ Goodfellow, I.; Bengio, Y.; Courville, A., *op. cit.* note 17, p. 164-325.

assumption exposes a structural mismatch between the conformity assessment architecture and the adaptive reality of post-deployment learning.

5. CONCLUSION

This article examined the presumption of conformity for medical AI under the AI Act through the lens of continuously learning deep-learning systems in genetic diagnostics. Because diagnostic DL software qualifies as a medical device under the MDR and therefore as a high-risk AI system under Article 6(1) AI Act and Annex I, Section A, the AI Act's enforcement architecture for such systems is structurally intertwined with sectoral medical device conformity assessment. Article 43(3) AI Act channels conformity assessment for Annex I systems through the applicable Union harmonisation act—in this case, the MDR—while maintaining the continued applicability of the substantive requirements in Title III, Chapter III, Section 2 AI Act. The practical significance of this design lies in the presumption of conformity: it implicitly assumes that sectoral conformity procedures, in combination with harmonised standards, can function as an equivalent and sufficiently comprehensive mechanism for demonstrating compliance with AI Act requirements.

The analysis shows that this equivalence assumption becomes contestable for continuous-learning genetic diagnostic systems. A first structural tension emerges at the level of MDR classification. Annex VIII and, in particular, Rule 11 are built around an *ex ante* assessment of intended purpose and foreseeable risks. Yet continuously learning systems are characterised by adaptive behaviour, probabilistic inference, and the potential for evolving performance characteristics after deployment. The phrase "may cause" in Rule 11 is calibrated to stable risk scenarios; it provides limited doctrinal traction for capturing dynamic risk evolution driven by retraining, dataset shifts,¹⁰⁸ or feedback loops.¹⁰⁹ As a consequence, classification can become unstable across time: a system may be assessed under one risk profile at market entry while exhibiting materially different error patterns or clinical impacts during real-world use. This instability matters because classification functions as a gateway to the applicable conformity assessment route and the intensity of regulatory controls.

Second, more fundamental tension concerns the temporal architecture of MDR conformity assessment. Across the routes provided under Article 52 MDR and

¹⁰⁸ Zhang *et al.*, *op. cit.* note 13, p. 1343-1345.

¹⁰⁹ Sculley, D. *et al.*, *op. cit.* note 16, p. 2506.

Annexes IX to XI, conformity assessment remains anchored in a snapshot logic. Technical documentation under Annex II is designed to evidence conformity at the time of submission; verification and validation tests relate to a defined system configuration; and quality management systems govern compliance through documented procedures and controlled change processes. These mechanisms presuppose that the certified configuration remains representative of the device's operational behaviour. By contrast, continuous-learning systems are defined by the possibility of model-state evolution after market placement. In genetic diagnostics, this divergence is amplified by the relational nature of genomic data and by the potential for changing inferential patterns over time. Even where the declared intended purpose remains formally unchanged, the practical scope and impact of a system's outputs may evolve, including through the emergence of secondary inferences that were not observable at the time of assessment.

Third, the comparative analysis of conformity assessment routes underscores that procedural completeness does not resolve the substantive blind spot for adaptive behaviour. Annex IX offers a process-oriented lifecycle framework and channels post-market changes through documentation, monitoring, and, where required, renewed conformity assessment. However, it does not constitute a mechanism for continuous substantive reassessment of evolving model behaviour as such. The regulatory logic is designed for manufacturer-initiated and ex ante bounded modifications; autonomous behavioural evolution sits uneasily within this paradigm. Annex X intensifies the static premise by tying compliance to an EU type-examination of a representative specimen, with an implicit expectation that certified characteristics remain stable. Annex XI, in turn, reinforces reliance on the certified type and, particularly in Part B, relies on unit-by-unit verification logic that is conceptually coherent for tangible devices but strained for centrally deployed software architectures characterised by ongoing update cycles and shifting operational states. Together, these routes reflect a coherent MDR conformity architecture—yet one that is structurally premised on stable device identity and point-in-time verification.

These findings have direct implications for the presumption of conformity under the AI Act. The presumption is functional only to the extent that harmonised standards and sectoral conformity procedures actually cover the relevant AI Act requirements for the system in question. For continuous-learning genetic diagnostics, the MDR's ex ante conformity logic risks producing a temporal and epistemic misalignment: extensive procedural obligations are maintained, yet the framework may not adequately capture the evolution of behaviour and risk that the AI Act seeks to govern through lifecycle-oriented requirements, including change management and post-deployment control of performance-relevant

modifications. This does not imply that the MDR is ineffective as product safety regulation, nor that continuous-learning systems are necessarily incompatible with the MDR. Rather, it clarifies that, in this domain, MDR conformity assessment may not be fully equivalent as an evidentiary basis for AI Act compliance where system behaviour is expected to evolve beyond what can be represented in a certification snapshot. This is particularly relevant because the presumption of conformity operates not merely as a procedural simplification, but as a mechanism that reallocates evidentiary confidence from direct regulatory scrutiny to standardised and sectoral assessment structures. Where those structures are not designed to observe or reassess behavioural evolution over time, the presumption risks becoming under-inclusive in relation to the very risks that distinguish adaptive AI systems from conventional medical software.

A forward-looking implication is that legal certainty will depend on clarifying how continuous learning is operationalised within the AI Act’s “substantial modification” logic and how this interacts with MDR change governance. Article 43(4) AI Act distinguishes between performance-relevant changes that require renewed conformity assessment and changes already accounted for within the original assessment. For genetic diagnostic software, the key regulatory task is therefore to specify what it means, in practice, to “take into account” adaptive behaviour *ex ante*, and how to define and evidence permissible change envelopes over time. While MDCG guidance and harmonised standards can provide procedural support, the central challenge is conceptual: aligning a stability-oriented conformity model with systems whose defining feature is behavioural evolution. Addressing this alignment is a precondition for ensuring that the presumption of conformity remains credible—both as a legal shortcut and as a substantive guarantee of safety and compliance for continuously learning medical AI.

REFERENCES

BOOKS AND ARTICLES

1. Erlich, Y.; Narayanan, A., Routes for Breaching and Protecting Genetic Privacy, *Nature Reviews Genetics*, 15, 2014, 409–421, doi:10.1038/nrg3723.
2. Feiler, L.; Forgó, N., *Kommentar KI-VO, EU-Verordnung über künstliche Intelligenz*, Verlag Österreich, Vienna 2024.
3. Forgó, N.; Prainsack, B., New AI regulation in the EU seeks to reduce risk without assessing public benefit, *Nature Medicine*, 30(5), 2024, 1235–1237, doi: 10.1038/s41591-024-02874-2.

4. Gama, J. *et al.*, A Survey on Concept Drift Adaptation, *ACM Computing Surveys*, 46(4), 2014, 1–37, doi:10.1145/2523813.
5. Goodfellow, I.; Bengio, Y.; Courville, A., *Deep Learning*, MIT Press, Cambridge (MA) 2016.
6. Herbst, T., Regulierung intelligenter Medizinprodukte, *ZfPC*, 2023.
7. Königshofer, W., Medical Device Law, in: Resch, R.; Wallner, F. (eds.), *Handbook of Medical Law*, 3rd ed., Manz, Vienna 2020, paras 137–151.
8. Ludvigsen, K.R.; Nagaraja, S.; Daly, A., The Intention; Requirements for Software as a Medical Device in EU Law, *SSRN Paper*, 2021, 1–38.
9. Schneeberger, D., Intelligente Medizinprodukte: Rechtsfragen am Schnittpunkt von DSGVO, MPVO und AI Act, *DaKo*, 1/2024, 4–7.
10. Sculley, D. *et al.*, Hidden Technical Debt in Machine Learning Systems, *Advances in Neural Information Processing Systems*, 2015, 2503–2511.
11. Seyyed-Kalantari, L. *et al.*, CheXclusion: Fairness Gaps in Deep Chest X-Ray Classifiers, *Pacific Symposium Biocomputing*, 26, 2021, 232–243.
12. Spiliopoulou, A. *et al.*, Genomic Prediction of Complex Human Traits: Relatedness, Trait Architecture and Predictive Meta-Models, *Human Molecular Genetics*, 24(14), 2015, 4167–4182, doi:10.1093/hmg/ddv145.
13. Stange, A.F.; Julian, E., Conformity Assessment of Medical Devices, *Journal of Market Access & Health Policy*, 14(1):4, 2026, doi:10.3390/jmahp14010004.
14. Wang, X. *et al.*, Inconsistent Performance of Deep Learning Models on Mammogram Classification, *Journal of the American College of Radiology*, 17(6), 2020, 796–803, doi:10.1016/j.jacr.2020.01.006.
15. Zhang, A. *et al.*, Shifting Machine Learning for Healthcare from Development to Deployment and from Models to Data, *Nature Biomedical Engineering*, 6(12), 2022, 1330–1345, doi:10.1038/s41551-022-00898-y.

LEGAL RULES

1. European Commission, Commission Notice – The Blue Guide on the implementation of EU product rules 2022, OJ C 247, 29 June 2022.
2. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L 2024/1689.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation), OJ L 2016/119.

4. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices (Medical Device Regulation), OJ L 2017/117.
5. Genetic Technology Act (Gentechnikgesetz – GTG), Federal Law Gazette (BGBl) No 510/1994, as amended by BGBl I No 8/2022.

NETWORK RESOURCES

1. COCIR – European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry, *Artificial intelligence in EU medical device legislation*, 2021, https://cocir.org/uploads/2021/10/COCIR_AI_in_EU_Medical_Device_Legislation_2021.pdf, accessed 21 February 2026.
2. European Commission, AI Act enters into force, 1 August 2024, https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en, accessed 21 February 2026.
3. European Commission, *Medical devices: Guidance document – Qualification and Classification of stand alone software (MEDDEV 2.1/6)*, July 2016, <https://ec.europa.eu/docsroom/documents/17921>, accessed 21 February 2026.
4. Medical Device Coordination Group (MDCG), *MDCG 2020-3 Rev.1 – Guidance on significant changes regarding the transitional provision under Article 120 MDR*, 2023, https://health.ec.europa.eu/document/download/5fb74e56-fd4c-4dae-9d24-78149edfe56b_en?filename=md_mdcg_2020_3_rev1_en.pdf, accessed 21 February 2026.
5. U.S. Food and Drug Administration (FDA), Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD): Discussion Paper and Request for Feedback, 2019, <https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf>, accessed 21 February 2026.

TABLE OF FIGURES

Figure 1: Input–output-based illustration of algorithmic change scenarios in AI-based genetic diagnostic systems under Annex IX MDR.

UDK: 004.738.5 : 34 (094.5)
316.774 : 17
Preliminary communication

Hannah Hafenscher, PhD student

Department of Innovation and Digitalisation in Law, University of Vienna, Austria

E-mail: hannah.hafenscher@univie.ac.at

ORCID: 0009-0005-9237-6471

CONSTITUTIONALIZING TERMS OF SERVICES? ARTICLE 14 (4) DSA AND THE BLURRING OF PUBLIC AND PRIVATE LAW IN THE EUROPEAN UNION

ABSTRACT

This contribution examines Article 14(4) of the Digital Services Act (DSA), which obliges online platform providers to apply and enforce their terms and conditions with "due regard" to the fundamental rights of all parties involved. The paper argues that this provision creates a novel framework in which private contractual autonomy coexists with values traditionally rooted in the public law domain. Even though the introduction of fundamental rights considerations into private platform governance can be seen as a step in the right direction, the absence of concrete criteria for resolving conflicts between the two results in legal uncertainty. By subjecting Article 14(4) DSA to a textual and systematic analysis, the contribution identifies three core ambiguities: the temporal scope of the due-regard obligation, its application to both illegal and lawful content, and the lack of a substantive balancing framework. The paper further argues that the principle of proportionality, while offering a doctrinal reference point, cannot be straightforwardly transposed into private platform governance. This tension is particularly acute in the context of AI-driven content moderation, where fully automated systems are structurally ill-suited to conduct the rights-sensitive, contextual balancing required by Article 14(4) DSA. The paper concludes that the EU legislator should have established clear substantive conditions limiting the use of fully automated moderation in cases where a genuine proportionality assessment is required and suggests that ex-ante human oversight combined with region-specific moderation frameworks developed in cooperation with public authorities, civil society, and local experts should be given prevalence. Employing doctrinal legal research complemented by normative and interdisciplinary analysis, the contribution seeks to clarify what this emerging regulatory model means for the future protection of fundamental rights in the digital public sphere.

Keywords: *Digital Services Act, Content Moderation, Fundamental Rights, Proportionality, AI-Driven Content Moderation*

1. INTRODUCTION

The governance of online content and communication has become one of the most pressing legal and societal questions of the digital age. Nowadays major platforms such as TikTok, Facebook and YouTube function as global intermediaries of speech and thus exercise a key role in the global information environment by deciding what kind of content their users can view online and how they are able to communicate.¹ The heated discourse surrounding the "censorship" by private operators, especially social media platforms, through their content moderation has developed to a major concern in the last years.² Private actors have the power to decide what information can be shared online, if it should be contextualized or even removed.³ Keeping in mind that freedom of expression constitutes one of the founding values within a democratic society⁴ it has been argued by numerous voices that the task of determining which content should be disseminated within online spaces should not be left to social media platform providers without harmonized rules and safeguards.⁵ It is particularly important to consider that content moderation decisions are often taken through automated systems⁶ or depend highly on internal moderation guidelines thus raising fundamental questions about accountability, fairness, and the protection of fundamental rights online. Especially with regards to the individual rights of users as well as the influence on democratic discourse, the issue becomes a significant one.⁷

¹ Botero Arcila, B.; Griffin R., Social media platforms and challenges for democracy, rule of law, and fundamental rights, Study requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, April 2023, p. 14, [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/743400/IPOL_STU\(2023\)743400_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/743400/IPOL_STU(2023)743400_EN.pdf), 19 December, 2025.

² Țucă, M., Digital Services Act: Is Article 14(4) Protecting Free Speech or Just Window Dressing?, January 2025, <https://www.conformia-hub.eu/blog/dsa-art14-free-speech>, 15 January, 2026.

³ Al-Zaman, S. Md., *Patterns and Trends of Global Social Media Censorship: Insights from 76 Countries*, Sage Journals, volume 87, 10/2024, p. 2f.

⁴ Council of Europe, *Freedom of Expression*, The European Convention on Human Rights, <https://www.coe.int/en/web/human-rights-convention/expression>, 26 November, 2025.

⁵ Jodanović, A., *The Digital Services Act Package: Protection of the Fundamental Rights of Digital Service Users in the European Union*, Regional Law Review, volume 5, 11/24, p. 52; Forsio, G., Geiger, C., *Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime*, European Law Journal, volume 29, 11/2023, p. 31f.

⁶ Griffin, R., Algorithmic Content Moderation Brings New Opportunities and Risks, October 2023, <https://www.cigionline.org/articles/algorithmic-content-moderation-brings-new-opportunities-and-risks/>, 04 November, 2025.

⁷ Quintais, P. J.; Appelman, N.; Ó Fathaigh, R., *Using Terms and Conditions to Apply Fundamental Rights to Content Moderation*, German Law Journal, volume 24, 11/2023, p. 884.

The so called "digital revolution"⁸ has exerted pressure on the European legislator to modernize the existing regulatory approaches and to build upon the e-Commerce Directive, especially regarding its liability privilege for platform operators that play "an intermediary role on the Internet."⁹ The proposed legal framework should enhance the responsibility of platform providers and improve the protection of users' rights. However, striking a balance to mitigate online harm, whilst ensuring fundamental rights like, the freedom of expression and information as well as the freedom to conduct a business is not an easy task.¹⁰

In response to these growing concerns the European Union adopted the Digital Services Act (DSA)¹¹ in October 2022, which entered into force in February 2024 for all platforms.¹² The DSA is a landmark framework within the EUs digital regulation seeking to recalibrate the relationship between users, platform providers, and society at large. To achieve its goals the DSA forms "a single set of rules" by imposing harmonized obligations on online intermediaries and platforms. Among its objectives are establishing "a safer digital space in which the fundamental rights of all users of digital services are protected", whilst also creating "a level playing field that fosters innovation, growth and competitiveness, both in the European Single Market and globally."¹³ Hence the key goals of this ambitious rulebook are to improve transparency, balance competing fundamental rights and create different mechanisms to protect users against illegal content, and disinformation.¹⁴

Among its most innovative features is Article 14 DSA, particularly its paragraph 4, which obliges online platforms to apply and enforce their terms of service with "due regard" to users' fundamental rights.¹⁵ This requirement marks a significant shift in EU law: contractual relationships between platforms and users are no longer governed solely by private autonomy but are explicitly infused with values

⁸Jodanović, *op. cit.* note 5, p. 49.

⁹ Wimmers, J., *The Out-of-Court Dispute Settlement Mechanism in the Digital Services Act: A Disservice to Its Own Goals*, Journal of Intellectual Property, Information Technology and E-Commerce Law, volume 12, 02/2022, p. 385.

¹⁰ Golunova, V.; Tas, S., *Guardians of Digital Rights: Exploring Strategic Litigation on Data Protection and Content Moderation in the EU*, Nordic Journal of European Law, volume 7, 01/2025, p. 57.

¹¹ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), OJ L 277 of 27 October 2022 (hereinafter: DSA).

¹² The Digital Services Act, Shaping Europe's digital future, October 2022, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>, 28 October, 2025.

¹³ *Ibid.*

¹⁴ *Ibid.*

¹⁵ Quintais, Appelman, Ó Fathaigh, *op. cit.* note 7, p. 894.

traditionally rooted in public law.¹⁶ Article 14 (4) DSA thus operates at the very point where public and private law intersect, raising foundational questions about the horizontal effect of fundamental rights,¹⁷ the impacts on private contractual autonomy, and the scope of the EU's competence to introduce fundamental right duties that apply to horizontal relationships through secondary legislation.¹⁸

This contribution argues that Article 14 (4) DSA creates a framework in which private contractual autonomy coexists with public-law values¹⁹, but without clear guidance as to how conflicts between the two should be resolved. The absence of concrete criteria on how platform providers should operationalize the balancing of competing fundamental rights in practice risks turning this assessment into a superficial "box-ticking" exercise by private actors²⁰ - thereby undermining the broader rights-protective ambitions of the DSA.²¹ While public-law principles such as proportionality may offer an initial doctrinal reference point, their transplantation into private platform governance,²² now increasingly shaped by AI-driven content moderation raises unresolved conceptual and institutional challenges.²³ By analyzing the doctrinal, institutional, and practical implications of Article 14 (4) DSA, the contribution seeks to illustrate how this provision challenges traditional boundaries between public and private law and explores what this emerging model of "hybrid speech governance"²⁴ may mean for the future protection of fundamental rights in the digital public sphere.

While earlier contributions in this field have primarily focused on the preliminary question of whether public-law values can be introduced into private-law relationships²⁵, and on how the horizontal effect of fundamental rights may exert

¹⁶ Mast, T.; Ollig, C., *The Lazy Legislature: Incorporating and Horizontalising the Charter of Fundamental Rights through Secondary Union Law*, European Constitutional Law Review, volume 19, 09/2023, p. 470.

¹⁷ Husovec, M., *Principles of the Digital Services Act*, 2024, p. 254.

¹⁸ Palumbo, A., *Disentangling the horizontalisation of fundamental rights in the Digital Services Act: What obligations for online intermediaries?*, Rivista di diritto dei media, volume 2, 10/2024, p. 104; Mast, Ollig, *op. cit.* note 16, p. 476.

¹⁹ Palumbo, *op. cit.* note 18, p. 102f.

²⁰ Quintais, Appelman, Ó Fathaigh, *op. cit.* note 7, p. 910.

²¹ Art. 1(1) DSA.

²² Wilman, F.; Kalèda, L. S.; Loewenthal, P., *The EU Digital Services Act*, Oxford University Press, 2024, p. 123; Quintais, Appelman, Ó Fathaigh, *op. cit.* note 7, p. 910.

²³ Hakami, A.; Tazel, R., *The Ethics of AI in Content Moderation: Balancing Privacy, Free Speech, and Algorithmic Control*, ResearchGate, 10/2024, p. 3.

²⁴ Schulz, W.; Ollig, C., *Hybrid Speech Governance: New Approaches to Govern Social Media Platforms under the European Digital Services Act?*, Journal of Intellectual Property, Information Technology and E-Commerce Law, volume 14, 02/2024, p. 561.

²⁵ Mast, Ollig, *op. cit.* note 16; Schulz, Ollig, *op. cit.* note 24; Palumbo, A.; Ducuing, C., *The Blurring of the Public-Private Dichotomy in Risk-Based EU Digital Regulation: Challenges for the Rule of Law*, SSRN Electronic Journal, 08/2025.

binding force on private actors²⁶, this contribution shifts the focus to the concrete balancing exercise that platform providers must undertake when confronted with competing interests. Particular attention is given to the role of the principle of proportionality in guiding this assessment. Against this background, the paper examines the extent to which reliance on fully AI-driven content moderation can be regarded as compatible with Article 14(4) DSA, which requires a contextual and rights-sensitive balancing of interests.

To achieve this objective, the paper employs doctrinal legal research (DLR) as its primary methodological approach, analyzing the relevant provisions of EU law, in particular the DSA and the Charter of Fundamental Rights of the European Union (CFR), together with the case law of the Court of Justice of the European Union (CJEU). To move beyond a purely descriptive account and to assess the normative adequacy of the current regulatory framework, the doctrinal analysis is complemented by a normative legal method, drawing on fundamental-rights principles developed in constitutional and human-rights jurisprudence. In addition, the analysis incorporates interdisciplinary research on artificial intelligence and automated decision-making in order to contextualize the legal assessment within the broader technological and socio-technical environment in which content moderation systems operate.

The contribution is grounded in the current state of academic research and draws on scientific literature in the fields of platform regulation, digital constitutionalism, and content moderation. Relevant academic literature was identified through established legal and interdisciplinary databases, including JIPITEC, Verfassungsblog, ResearchGate, Westlaw, Beck-Online, SSRN, Tech Policy Press and Google Scholar. Technical and interdisciplinary research on artificial intelligence and automated decision-making was additionally consulted through databases such as IEEE Xplore and the ACM Digital Library. EU legislation was accessed via the official EUR-Lex database, while judgments of the Court of Justice of the European Union were consulted through the Court's official website (curia.europa.eu).

2. THE NEED TO INTEGRATE PUBLIC-LAW VALUES INTO PRIVATE RELATIONSHIPS

To contextualize the issue outlined above, it should be noted that platform providers are still private actors and that the relationship between platforms and

²⁶ Quintais, Appelman, Ó Fathaigh, *op. cit.* note 7.

users is of contractual nature, with the terms and conditions forming the basis. In principle, fundamental rights instruments, such as the Charter of Fundamental Rights (CFR) traditionally only apply to relationships between individuals and states and do not govern vertical relationships between private parties.²⁷ Rights, like the freedom of expression and information, do not oblige private entities to tolerate all types of information in their digital spaces. Within the scope of contractual autonomy, platform providers can implement rules that are more restrictive than those imposed by state bodies.²⁸ However, caution is advised when it comes to large social media platforms such as TikTok, Instagram and YouTube. These private providers occupy a dominant position in contemporary digital society.²⁹ This phenomenon can be explained by the significant power imbalance between large platform providers and their users. While providers of online platforms can largely determine their internal rules unilaterally, users usually have no choice but to accept these requirements. The platform's policies thus ultimately shape the conditions under which online users can participate in the online discourse.³⁰ They hold a monopoly within the digital communication sphere, as it is almost impossible for users to switch to another platform offering analogous communication services without experiencing personal downsides, if they are unwilling to agree to the terms and conditions.³¹ For this reason, major platform operators are often referred to as "intermediaries", and in my opinion, rightly so. They occupy an intermediate position between the state and society because they have the power to control and influence digital infrastructure.³² Importantly, they not only have the ability to influence the structure and functioning of the informational environment itself, but also how their users are able to communicate within it. Consequently, the restrictions imposed by platform providers in their terms and conditions can have a significant impact on users' fundamental rights, including freedom of expression and freedom of information, as well as the rights to privacy and data protection. At the same time, providers are required to moderate content distributed on their platform, which may lead to the removal, restriction, or filtering of vast amounts of allegedly unlawful online material. Such

²⁷ Quintais, Appelman, Ó Fathaigh, *op. cit.* note 7. 882; Senfleben, M., Human Rights Outsourcing and Reliance on User Activism in the DSA, February 2024, <https://verfassungsblog.de/human-rights-outsourcing-and-reliance-on-user-activism-in-the-dsa/>, 31 December, 2025.

²⁸ Pöschl, M., *Neuvermessung der Meinungsfreiheit*, in: H. Koziol (ed.), *Tatsachenmitteilungen und Werturteile: Freiheit und Verantwortung*, Jan Sramek Verlag, Vienna 2018, p. 57; Schulz, Ollig, *op. cit.* note 24, p. 562f.

²⁹ Palumbo, *op. cit.* note 18, p. 103.

³⁰ Quintais, Appelman, Ó Fathaigh, *op. cit.* note 7, p. 883.

³¹ Pöschl, *op. cit.* note 28, p. 57.

³² *Ibid.*, p. 59.

measures directly affect the rights of those users that created the content.³³ Considering that the online environment has become a primary channel for exercising the right to freedom of expression and information,³⁴ it is unsurprising that the protection of these rights constitutes a central element within the DSA's framework.³⁵

From a broader constitutional perspective, the regulatory intervention of the EU legislator in the contractual relationship between platform providers and users can also be understood in light of a well-established concept in democratic welfare states: the justification of setting limits to the freedom of contract³⁶ to ensure that the factually weaker contractual party can "fully enjoy their freedom of self-determination."³⁷ In areas such as consumer or labor law, contractual autonomy has long been complemented by protective legislative intervention in cases where structural inequalities could possibly undermine contractual autonomy.³⁸ Although traditional welfare-state objectives³⁹ are not directly implicated in the relationship between digital platforms and their users, analogous reasoning nonetheless supports the argument that stronger regulatory intervention at EU level is needed in this context.

The asymmetry of economic power and communicative control exercised by large platforms affects not only the private interests of individual users but also their ability to effectively exercise their freedom of expression,⁴⁰ which presents a cornerstone of democratic society.⁴¹ Consequently, legislative intervention that limit platform autonomy and discretion may be justified not merely as market

³³ Geiger, C.; Frosio, G., Izyumenko, E., *Intermediary Liability and Fundamental Rights*, SSRN Electronic Journal, 06/2029, p. 3; Wilman, Kalèda, Loewenthal, *op. cit.* note 22, p. 122.

³⁴ *Sanchez v. France* (GC), App. no. 45581/15, ECtHR, 15 May 2023, para. 184.

³⁵ Mast, Ollig, *op. cit.* note 16, p. 468f.

³⁶ Hesselink, M. W., *The Values Underlying the Draft Common Frame of Reference: What Role for Fairness and "Social Justice"?*, Study No. PE 408.312, European Parliament, Directorate General Internal Policies of the Union, 2008, p. 12f.

³⁷ Mak, C., *Fundamental Rights in European Contract Law: A Comparison of the Impact of Fundamental Rights on Contractual Relationships in Germany, the Netherlands, Italy and England*, Kluwer Law International, Alphen aan den Rijn 2007, p. 33.

³⁸ Mak, V., *Redefining Equality in European Contract Law: Protecting Consumer Interests in a Post-Consumer Society*, European Law Open, 2024, p. 564; Tedoradze, I., *The Principle of Freedom of Contract, Pre-Contractual Obligations* *Legal Review English, EU and US Law*, European Scientific Journal, volume 13, 02/2017, p. 63.

³⁹ See for overview: Güler, M. A., *The Concept of the Welfare State and Typologies of Welfare Regimes: A Review*, *Problemy Polityki Społecznej*, volume 47, 4/2019, p. 115ff.

⁴⁰ Quintais, Appelmann, Ó Fathaigh, *op. cit.* note 7, p. 882f.

⁴¹ Council of Europe, *Freedom of Expression*, ECHR Toolkit, <https://www.coe.int/en/web/echr-toolkit/la-liberte-dexpression>, 16 February, 2026.

regulation but as a means of safeguarding fundamental rights and protecting the democratic public sphere. Against this background, Article 14(4) DSA can be seen as an expression of this broader constitutional logic. This logic translates the protection of the weaker contracting party and the preservation of democratic discourse into obligations for the private regulation of online communication.

3. ARTICLE 14(4) DSA: THE "DUE REGARD" OBLIGATION

3.1. Overview of Article 14 DSA

Article 14 DSA constitutes a novel regulatory intervention in the governance of intermediary services by introducing binding rules on how internal platform policies, namely the terms and conditions ought to be applied and enforced.⁴² Within the meaning of the DSA, the terms and conditions as a concept encompass "all clauses, irrespective of their name or form, which govern the contractual relationship between the provider of intermediary services and the recipients of the service."⁴³ While the Regulation continues to recognize the principle of freedom of contract⁴⁴, Article 14 DSA reflects a clear legislative intent to rebalance the structural power asymmetry inherent in the relationship between platform providers and their users.⁴⁵ It does so by imposing a set of obligations aimed at enhancing transparency, strengthening the protection of users' rights, and mitigating the risk of "unfair or arbitrary outcomes"⁴⁶ in the application and enforcement of platform rules.

Article 14 DSA is structured into distinct normative components that impose different types of obligations on platform providers.⁴⁷ Two sets of obligations within Article 14 DSA can be distinguished: procedural and substantive safeguards.⁴⁸ The procedural obligations are set out in paragraphs 1 to 3 and 5 to 6. They establish primarily transparency-oriented duties, requiring platforms to draft, communicate, and update their terms and conditions in a clear, accessible,

⁴² Husovec, *op. cit.* note 17, p. 254.

⁴³ Art. 3 (u) DSA.

⁴⁴ Recital 45 DSA.

⁴⁵ Mast, Ollig, *op. cit.* note 16, p. 470.

⁴⁶ Recital 45 DSA.

⁴⁷ Quintais, Appelman, Ó Fathaigh, *op. cit.* note 7, p. 892.

⁴⁸ Palumbo, *op. cit.* note 18, p. 102.

and comprehensible manner.⁴⁹ The aim of this component is to safeguard users against arbitrary, inconsistent, and non-transparent content moderation practices.⁵⁰ By contrast, Article 14(4) DSA introduces substantive obligations by addressing how online intermediaries should apply and enforce their terms and conditions, thus this component governs how internal platform rules are to be implemented in practice⁵¹ and obliges platform providers to give due consideration to users' fundamental rights in the exercise of their activities.⁵²

The following section provides a textual interpretation of Article 14(4) DSA, read in conjunction with the relevant recitals. Given that the objective of this chapter is to examine the role and effectiveness of Article 14(4) DSA to protect fundamental rights online effectively, the analysis will focus specifically on this provision. The other paragraphs of Article 14 DSA will be considered insofar as they inform and complement the interpretation of paragraph 4. However, their autonomous interpretation falls outside the scope of this contribution.

3.2. Textual and Systematic Analysis of Article 14 (4) DSA

When looking at Article 14 DSA from the perspective of fundamental rights, the normative core of the provision is contained in its paragraph 4. It requires platform providers to "act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved."⁵³ Article 14(4) DSA thus establishes an explicit obligation for platform providers to take fundamental rights and legitimate interests into account when applying and enforcing their terms and conditions, marking a significant departure from a purely contractual conception of platform governance.⁵⁴

Despite its apparent influence of the provision on content moderation practices, the precise scope of Article 14(4) DSA remains contested in academic literature. First, it is unclear whether the obligation to take fundamental rights into account applies solely at the stage of applying and enforcing existing terms and conditions,

⁴⁹ Fasel, M.; Weerts, S., *Can Facebook's Community Standards Keep up with Legal Certainty? Content Moderation Governance under the Pressure of the Digital Services Act*, Policy & Internet, volume 16, 05/2024, p. 589.

⁵⁰ Palumbo, *op. cit.* note 18, p. 102.

⁵¹ Quintais, Appelman, Ó Fathaigh, *op. cit.* note 7, p. 893f.

⁵² Palumbo, *op. cit.* note 18, p. 102.

⁵³ Quintais, Appelman, Ó Fathaigh, *op. cit.* note 7, p. 894.

⁵⁴ Ruschemeier, H.; Quintais, J. P., *Fundamental Rights in Out-of-Court Dispute Settlement under the Digital Services Act*, SSRN Electronic Journal, 12/2025, p. 11.

or whether it also extends to the drafting and design of those terms.⁵⁵ When adopting a strictly textual interpretation of Article 14(4) DSA it could be argued that platform providers are not required to take fundamental rights into account during the drafting phase of their platform policies, as the provision explicitly refers only to the application and enforcement of the terms and conditions. On this reading, the content and design of those rules would fall entirely within the platform's discretion, and fundamental rights would only become relevant once the rules are implemented in practice, that is, when they are applied and enforced vis-à-vis users. Such a limited interpretation would significantly narrow the scope of the due-regard obligation, confining it to the content moderation activity as such and excluding previous normative decisions taken by the platform providers, enshrined in their internal rules.⁵⁶ Second, the provision does not clarify whether its obligations are limited to content moderation decisions taken on the basis of violations of the platform's terms and conditions, or whether they also apply to decisions characterizing certain information as illegal content.⁵⁷ While the recitals remain silent on this point, the dominant position in the literature, which with I would agree, holds that Article 14 DSA extends to both illegal and lawful content.⁵⁸ This view is supported by the DSA's structure and regulatory objectives, which justify applying the fundamental-rights obligation in Article 14(4) to decisions concerning illegal content.⁵⁹ Third, and possibly the most crucial aspect to consider given the variety of different interest at stake, Article 14(4) DSA misses the opportunity to introduce concrete criteria, that guide platform providers how they should balance competing fundamental rights in practice.⁶⁰ Art 14 (4) does not set out any guidelines that could help, when determining the substantive scope of the obligation. By relying on the notion of "due regard," the provision fails to specify the intensity of the fundamental rights assessment required of platform providers within their content moderation practices.⁶¹ It is debated whether Article 14(4) imposes a primarily a duty of general nature to include procedural and systemic safeguards into their internal policies and enforcement framework or whether it mandates a case-by-case balancing of competing rights and interests in individual moderation decisions.⁶²

⁵⁵ Ruschemeier, Quintais, *op. cit.* note 54, p. 11; Husovec, *op. cit.* note 17, p. 254.

⁵⁶ Schulz, Ollig, *op. cit.* note 24, p. 575.

⁵⁷ Ruschemeier, Quintais, *op. cit.* note 54, p. 24.

⁵⁸ Quintais, Appelman, Ó Fathaigh, *op. cit.* note 7, p. 892; Mast, T.; Kettemann, M. C.; Schulz, W., DSA Art. 14 Allgemeine Geschäftsbedingungen, in: Mast, T.; Kettemann, M. C.; Dreyer, S.; Schulz, W. (eds.), *Digital Services Act, Digital Markets Act, 2024*, para. 53ff. cited in: Ruschemeier, Quintais, *op. cit.* note 54, p. 24.

⁵⁹ Ruschemeier, Quintais, *op. cit.* note 54, p. 24.

⁶⁰ Quintais, Appelman, Ó Fathaigh, *op. cit.* note 7, p. 910.

⁶¹ Schulz, Ollig, *op. cit.* note 24, p. 576.

⁶² Ruschemeier, Quintais, *op. cit.* note 54, p. 22; Husovec, *op. cit.* note 17, p. 255.

A closer reading of Recital 47 provides important, but also incomplete, guidance on some of these questions. Unlike the wording of Article 14(4), the recital explicitly refers not only to the application and enforcement of restrictions, but also to their "designing" suggesting a broader temporal scope that may encompass the process of drafting the terms and conditions.⁶³ This interpretation is in my opinion clearly in line with the DSA's general architecture and objectives.⁶⁴ Particularly when one keeps in mind that platform providers might introduce stricter restrictions on the information that users can share in their terms and conditions. They can deny content that is not classified as illegal by law, which in turn could lead "suppression of lawful content"⁶⁵ if the fundamental rights of the users are not considered during the drafting phase of the terms and conditions. Moreover, Recital 47 DSA refers only to the "rights and legitimate interests of the recipients of the service" whereas Article 14(4) DSA requires intermediary services to pay due regard to "the rights and legitimate interests of all parties involved". This divergence raises the question of whether Article 14(4) DSA is intended to protect a wider range of interests, such as those of the platform providers themselves, content creators, or other affected third parties beyond the direct user of the platform.⁶⁶ However, in this context, reference should be made to the established case law of the Court of Justice of the European Union, according to which recitals in the preamble of EU secondary legislation have "no binding legal force and cannot be relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner clearly contrary to their wording."⁶⁷ It can therefore be assumed that, through the recital, the EU legislator intended to place particular emphasis on the protection of the "recipients of the service," whose rights are likely to be most directly affected by many content-moderation decisions. Nevertheless, the explicit reference to "all parties involved" in the provision indicates that the EU legislator recognizes that platform operators themselves enjoy fundamental rights in the context of content moderation.⁶⁸ This, in turn, raises the complex question of how platform providers are to balance these potentially competing fundamental rights

⁶³ Husovec, *op. cit.* note 17, p. 254; Wilman, Kalèda, Loewenthal, *op. cit.* note 22, p. 122.

⁶⁴ Art. 1 (1) DSA states "[...] setting out harmonised rules for a safe, predictable and trusted online environment [...] in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected." Art. 1(1) DSA. The protection would in my opinion not be effective if the requirement to take fundamental rights into account does not apply to the drafting phase, as providers would retain full discretion to set rules restricting content in a manner incompatible with fundamental rights.

⁶⁵ Quintais, Appelmann, Ó Fathaigh, *op. cit.* note 7, p. 884f.

⁶⁶ Schulz, Ollig, *op. cit.* note 24, p. 575f.

⁶⁷ Case C-136/04, *Deutsches Milch-Kontor GmbH v. Germany*, ECR I-10095, 6 October 2005, para. 32, with reference to Case C-162/97, *Nilsson and Others*, ECR I-7477, 19 November 1998, para. 54; Case C-308/97, *Manfredi*, ECR I-7685, 25 June 1998, para. 30.

⁶⁸ Schulz, Ollig, *op. cit.* note 24, p. 575.

in practice. Additionally, Recital 47 extends the behavioral standard imposed on platforms by requiring them to act not only in "a diligent, objective and proportionate", but also in "a non-arbitrary and non-discriminatory manner". In doing so, the DSA, even if only through a recital, effectively incorporates not only the principle of proportionality, but also obligation of equal treatment, both traditionally only imposed on state actors as a manifestation of the rule of law, into the private governance exercised by platform operators. How these public-law principles are to be operationalized in the context of modern private content-moderation practices remains unclear.⁶⁹

The purpose of the following sections is therefore to examine how platform providers operationalize the balancing of competing fundamental rights and to assess whether the current approach is adequate, particularly in light of the principle of proportionality.

4. THE BALANCING ACT: FUNDAMENTAL RIGHTS IN PRIVATE HANDS

Although the precise conditions under which EU fundamental rights may apply in relationships between private parties, and thus produce horizontal effect, remain the subject of debate⁷⁰, the case law of the CJEU has clarified that the Charter itself, particularly Article 51(1) CFR does not, as a general rule, preclude "such a possibility."⁷¹ It would go beyond the scope of this contribution to argue comprehensively for or against the horizontal effect of EU fundamental rights. Moreover, in the specific context of Article 14(4) DSA, this debate is, in my opinion, of limited practical relevance, since the EU legislator has expressly embedded at least some form of fundamental rights effect, whether understood as a substantive obligation or as a "declaratory acknowledgment"⁷² of the nature of fundamental rights, applicable to private entities within the DSA's normative framework.⁷³ What seems more relevant to discuss in this context is the extent to which the EU legislator must pre-determine a "substantive framework" governing

⁶⁹ *Ibid.*, p. 574.

⁷⁰ Wendel, M., *Taking or Escaping Legislative Responsibility? EU Fundamental Rights and Content Regulation under the DSA*, in: Ungern-Sternberg, A. et al. (eds.), *Content Regulation in the European Union: The Digital Services Act*, Institut für Recht und Digitalisierung, Trier 2023, p. 66.

⁷¹ Joined Cases C-569/16 and C-570/16, *Stadt Wuppertal v. Bauer and Willmeroth v. Broßonn*, EU:C:2018:871, 6 November 2018, para. 87.

⁷² Wendel, *op. cit.* note 70, p. 78.

⁷³ Husovec, *op. cit.* note 17, p. 254.

how the balancing of competing fundamental rights is to be operationalized by such private actors.⁷⁴

As discussed above, Article 14(4) DSA explicitly mandates online intermediaries to integrate fundamental rights considerations into their terms and conditions and moderation activities.⁷⁵ The inherent power imbalance between platform providers and users can in principle also be seen as good reason for the EU legislator to incorporate concepts, traditionally rooted in public law into this horizontal relationship.⁷⁶ As discussed earlier in this paper, platform providers can unilaterally impose major restrictions on the way individuals are able to communicate within their services. As a result, their capacity to affect fundamental rights is comparable to that of state authorities.⁷⁷ In the EU legal order, conflicts between fundamental rights must be resolved in accordance with the principle of proportionality, which requires a careful balancing of competing rights and interests.⁷⁸ In its original conception, proportionality is a principle developed for state action. It is designed to mitigate the power asymmetry between the state and its citizens by limiting the state's ability to interfere with fundamental rights.⁷⁹ However, it can and has been argued that the obligation to conduct a proportionality test originally developed to bind state actors, can be applied to online intermediaries, given they obtain a similar dominant power position.⁸⁰ This approach is further reinforced by the fact that Article 14(4) DSA itself explicitly requires platform providers "to act in a [...] proportionate manner" when moderating content.⁸¹ However, it is unclear to what extent platform operators can effectively be required to respect users' fundamental rights, given that they are themselves beneficiaries of fundamental rights protection.⁸² Since private actors have traditionally only been able to invoke their fundamental rights against state actors, the binding effect of fundamental rights in the private sphere cannot be fully equated with those of state actors. This distinction is also expressly reflected in the DSA framework, as Article 14(4) refers to the fundamental rights of "all parties involved," thereby encompassing the fundamental rights of platform

⁷⁴ Wendel, *op. cit.* note 70, p. 70.

⁷⁵ Palumbo, *op. cit.* note 18, p. 104.

⁷⁶ Teubner, G.; Golia, A. Jr., *Societal Constitutionalism in the Digital World: An Introduction*, MPIL Research Paper Series No. 2023-11, Max Planck Institute for Comparative Public Law and International Law, 2023, p. 8. <https://www.jura.uni-frankfurt.de/146712046/DigitalConstitutionalismIntroductionENG2023.pdf>, 8 February, 2026; Palumbo, *op. cit.* note 18, p. 108.

⁷⁷ Palumbo, *op. cit.* note 18, p. 108.

⁷⁸ Palumbo, *op. cit.* note 18, p. 109; Wendel, *op. cit.* note 70, p. 65.

⁷⁹ Schulz, Ollig, *op. cit.* note 24, p. 574.

⁸⁰ Palumbo, *op. cit.* note 18, p. 109f.

⁸¹ Schulz, Ollig, *op. cit.* note 24, p. 574.

⁸² *Ibid.*, p. 572.

providers themselves.⁸³ By enabling platform providers to weigh their own economic fundamental rights against those of other private parties,⁸⁴ the EU legislator extends constitutional balancing concepts into private governance. Article 14(4) DSA thus embodies "a new form of hybrid regulation." Through this framework, the EU legislator entrusts platform providers to regulate fundamental rights of other private parties, namely users.⁸⁵

In principle, such an approach may appear sensible to a certain extent, as the legislator leaves service providers some flexibility to meet their own economic needs. Fully regulating the internal functioning of private operators, could interfere with their freedom of contract and their freedom to conduct a business, protected under Article 16 CFR, and any such interference itself would have to comply with the requirements of Article 52 (1) CFR.⁸⁶ However, it can be argued that the EU legislator should nonetheless have established a more clearly defined "substantive framework" governing how the balancing of competing fundamental rights is to be carried out in practice. By doing so, the legislator could have meaningfully constrained the interpretative discretion currently enjoyed by online intermediaries, while still respecting their economic freedoms.⁸⁷ However, the EU legislator refrained from providing a clear normative framework or standardized methodology on how platforms should balance competing rights, offering instead limited guidance for the application of Article 14(4) DSA.⁸⁸ This results in a broad margin of discretion for platform providers to determine which restrictions they introduce in their terms and conditions and how they enforce them. Given that platforms are empowered not only to prohibit illegal content but also to restrict expression that is lawful yet considered undesirable the EU legislator should, at a minimum, have established clearer standards concerning the normative requirements and substantive boundaries of such restrictions.⁸⁹ Particularly in light of the increasing reliance on AI-driven content moderation⁹⁰, the absence of a coherent regulatory framework that governs how platform providers must balance different interests becomes apparent. The question of how an effective, transparent, and fair balancing of competing fundamental rights can be achieved in content moderation systems that rely heavily and, in some cases, fully on

⁸³ *Ibid.*, p. 574f.

⁸⁴ *Ibid.*, p. 575.

⁸⁵ Mast, Ollig, *op. cit.* note 16, p. 470.

⁸⁶ Wendel, *op. cit.* note 70, p. 79f.

⁸⁷ *Ibid.*, p. 81.

⁸⁸ Mast, Ollig, *op. cit.* note 16, p. 470.

⁸⁹ Wendel, *op. cit.* note 70, p. 81.

⁹⁰ Vargas Penagos, E., *Platforms on the Hook? EU and Human Rights Requirements for Human Involvement in Content Moderation*, Cambridge Forum on AI: Law and Governance, volume 1, 2025, e23, p. 7.

automated, algorithmic decision-making remains largely unresolved. At the core of the problem lies a structural tension. AI-driven content moderation can significantly enhance the efficient detection and mitigation of misinformation, hate speech, and other forms of unlawful or harmful content that may infringe the fundamental rights of affected individuals.⁹¹ Furthermore, reliance on fully automated moderation may reduce the need for human moderators, whose work routinely entails prolonged exposure to disturbing content, significant psychological strain, and employment conditions marked by low pay and limited labor protection.⁹² At the same time, however, the use of fully or largely autonomous moderation systems carries a considerable risk of removing or restricting lawful and legitimate expression, thereby potentially infringing the fundamental rights of other users.⁹³ This dynamic substantially complicates the balancing exercise that platform operators must conduct under Article 14 (4) DSA. It therefore raises the question whether it is proportionate to rely on algorithmic content moderation as a means of protecting the fundamental rights of certain individuals while simultaneously accepting the risk that such systems may unduly interfere with the rights and interests of others. In my view, this is precisely the point at which the EU legislator should have intervened by establishing a legal framework that differentiates between the various contexts and risk levels in which automated content moderation is employed.

In the following chapter, this contribution seeks to outline a set of criteria aimed at clarifying the circumstances in which reliance on automated content moderation may be regarded as proportionate from a human-rights perspective, as well as those in which it may not. For the sake of clarity, the term "automated content moderation" is used here to refer to its most recent development namely, the proactive monitoring of content through the use of artificial intelligence (AI) tools, in particular large language models (LLMs).⁹⁴

5. ASSESSING THE PROPORTIONALITY OF ALGORITHMIC CONTENT MODERATION

AI-driven content moderation can indeed be a highly useful tool in certain contexts - emphasis here is deliberately placed on certain. In particular, automated systems can be effective in tasks of detection, such as identifying images containing clearly illegal or offensive symbols, which can often be reliably recognized through

⁹¹ Hakami, Tazel, *op. cit.* note 23.

⁹² Griffin, *op. cit.* note 6.

⁹³ Hakami, Tazel, *op. cit.* note 23.

⁹⁴ Griffin, *op. cit.* note 6.

pattern-matching techniques. In such cases, algorithmic moderation may contribute to the efficient enforcement of platform rules and legal obligations.⁹⁵ However, when moderation decisions move beyond detection and towards determining what constitutes acceptable speech on a platform, the nature of the task fundamentally changes.⁹⁶ Especially in cases involving speech that is not unlawful but nevertheless considered harmful or undesirable⁹⁷, moderation necessarily involves normative value judgments. These decisions reflect choices about platform values and about where the boundaries of acceptable expression are to be drawn within a privately governed communication space.⁹⁸ As explained above, the principle of proportionality and with it the careful balancing of competing rights forms a central pillar of the due diligence obligation imposed on platform providers by Art 14 (4) DSA.⁹⁹ It requires that any encroachment on the fundamental rights of users imposed in the terms and conditions must be appropriate and necessary to achieve the underlying objectives.¹⁰⁰ Accordingly, where the proportionality of a moderation measure is in doubt, a substantive value judgment becomes a prerequisite for determining whether or not this restriction (e.g. removal of certain content or account blocking) should be imposed on a user. Algorithms, however, are not capable of making value judgments in this sense; rather, they generate statistical predictions based on patterns in training data.¹⁰¹ Consequently, AI tools are often unable to capture linguistic nuance or account for diverse cultural contexts.¹⁰² For this reason, such systems alone are not yet sophisticated enough to conduct the kind of balancing exercise required under Article 14(4) DSA. Delegating the constitutional balancing exercise and normative decision-making not only to private operators but indirectly to automated systems enhances the risk of obscuring the underlying value choices and undermining the careful balancing of fundamental rights that proportionality requires.

In this context, it is important to emphasize that the DSA does not prohibit fully automated content moderation at any stage. Instead, the DSA introduces certain

⁹⁵ Hendrix, J., *AI Snake Oil: Separating Hype from Reality*, Tech Policy Press, 29 September 2024, <https://www.techpolicy.press/ai-snake-oil-separating-hype-from-reality/>, 30 January, 2026.

⁹⁶ *Ibid.*

⁹⁷ Wendel, *op. cit.* note 70, p. 83.

⁹⁸ Hendrix, *op. cit.* note 95.

⁹⁹ Schulz, Ollig, *op. cit.* note 24, p. 574.

¹⁰⁰ Penagos, *op. cit.* note 90, p. 19.

¹⁰¹ Nishant, R.; Schneckenberg, D.; Ravishankar, M. N., *The Formal Rationality of Artificial Intelligence-Based Algorithms and the Problem of Bias*, Journal of Information Technology, volume 39, 1/2024, p. 21.

¹⁰² Gavi, K., *Ethical Challenges in AI-Powered Hate Speech Detection: Balancing Automated Moderation and Dataset Creation*, ResearchGate, January 2025, p. 1.

safeguards, such as transparency requirements concerning the use of algorithmic systems (Articles 14(1), 15(1), 16(6), and 17(3)(c) DSA).¹⁰³ It has even been assumed that, with the adoption of the DSA, the European Union has further incentivized platforms to deploy increasing levels of automated moderation.¹⁰⁴ However, in situations where the balancing of competing rights is required, fully automated moderation appears to stand in fundamental tension with the objective that Article 14(4) DSA seeks to achieve, namely careful balancing of competing fundamental rights. In my view, the mere introduction of safeguards is insufficient, as it leaves the underlying decision of whether to rely on fully automated content moderation entirely to the discretion of platform providers. This is highly problematic, as platform operators, being private entities, are not primarily oriented towards the protection of fundamental rights but rather toward the generation of income and revenue. If the underlying decision to rely on fully automated content moderation systems is left entirely to private providers, the decisive factors are likely to be considerations of efficiency and cost, rather than the effective protection of fundamental rights.¹⁰⁵ Since automated content moderation is in most scenarios very attractive from an economic point of view due to the possibility of speeding up large-scale processes¹⁰⁶, platform providers will most likely tend to favor content moderation systems that are less costly rather than less intrusive.¹⁰⁷ Moreover, algorithmic tools used to determine what information can and cannot be shared on a platform are likely to prioritize the platform's commercial interests over broader public interests.¹⁰⁸ However, particularly in this context, such practices may risk endangering not only the rights of individuals but also those of society at large. The task of moderating online content as such raises distinct democratic challenges not only due to the chilling effects it can have on fundamental rights, but also due to its capacity to influence public discourse and democratic processes.¹⁰⁹ The decision how and to what extent this process should be automated through the use of AI should therefore not be left solely to the discretion and commercial interests of platform providers, but instead must be designed and deployed in a transparent manner and in full consideration of human rights.¹¹⁰ Article 14(4) DSA implicitly requires moderation grounded in the principle of proportionality. However, the absence of

¹⁰³ *Ibid.*, p. 12.

¹⁰⁴ Kayyali, D., *An Advocate's Guide to Automated Content Moderation*, Tech Policy Press, 12 February 2025, <https://www.techpolicy.press/an-advocates-guide-to-automated-content-moderation/>, 10 February 2026.

¹⁰⁵ Senfleben, *op. cit.* note 27, p. 2.

¹⁰⁶ Penagos, *op. cit.* note 90, p. 22.

¹⁰⁷ Senfleben, *op. cit.* note 27, p. 3; Griffin, *op. cit.* note 6.

¹⁰⁸ Griffin, *op. cit.* note 6.

¹⁰⁹ Penagos, *op. cit.* note 90.

¹¹⁰ Kayyali, *op. cit.* note 104.

substantive legislative criteria combined with the growing reliance on AI-driven content moderation creates a structural gap that risks undermining effective protection of fundamental rights and raises broader societal challenges. At this juncture, the EU legislator should have intervened by establishing clear substantive conditions limiting the use of fully automated moderation in situations where a normative value judgment is required and the proportionality of a restriction is at stake.

6. CONCLUSION

This contribution does not suggest that the EU legislator should exclude the use of AI in content moderation altogether. Such an approach would hardly be feasible given the vast volume of content generated on online platforms every second. Rather, what is required is a clear normative framework that differentiates between the various use cases in which automated moderation is deployed. As discussed above, AI-driven moderation can be highly effective in situations where no further contextualization or value judgment is required. However, where a genuine proportionality assessment is necessary to determine the legitimacy of certain content, AI-driven moderation should be combined with meaningful expert oversight and supported by an adequate number of human moderators.¹¹¹

In my view, the DSA does not explicitly endorse such an approach. Instead, it appears to follow an ex-post model for constraining AI-driven moderation. Human oversight becomes mandatory only at a later procedural stage, notably through the internal complaint-handling mechanisms under Article 20 DSA¹¹² and the external dispute-settlement procedures provided for in Article 21 DSA¹¹³. Particularly in the context of fully automated moderation, this structure is problematic. It effectively places the burden on users to challenge moderation decisions in order to obtain access to human review. By contrast, Article 14(4) DSA can be understood as implicitly requiring human oversight in the moderation process at an earlier stage, namely, prior to the adoption of the moderation decision whenever

¹¹¹ European Center for Not-for-Profit Law (ECNL), *Algorithmic Gatekeepers: The Human Rights Impacts of LLM Content Moderation — Executive Summary*, 2025, https://ecnl.org/sites/default/files/2025-04/ECNL_LLM_CM_Executive%20Summary_2025.pdf, 4 February, 2026.

¹¹² Article 20(6) DSA explicitly provides that decisions adopted by platform providers within the internal complaint-handling mechanism must be “taken under the supervision of appropriately qualified staff, and not solely on the basis of automated means.” This provision indicates that fully automated decision-making in the context of internal complaints is prohibited and that human oversight is expressly required.

contextual balancing is necessary. In such cases, the EU legislator should therefore have adopted an ex-ante model of human oversight for AI-driven content moderation. The argument that moderation work is inherently too psychologically demanding for human moderators is likewise unconvincing to promote full reliance on AI tools. Rather, it is primarily the inadequate working conditions, such as excessive working hours and low wages, that render this work inhumane. The appropriate response should therefore be to improve the working conditions of human moderators, including reasonable limits on working time and fair remuneration, and to support them through collaboration with appropriately trained experts who can provide meaningful guidance. In this way, human moderators could become a valuable and sustainable resource for platform providers, rather than being replaced by AI-driven systems.

One of the central challenges associated with automated moderation tools lies in their frequent inability to capture contextual and linguistic nuance. Yet the balancing of competing fundamental rights often requires careful consideration of cultural context, linguistic particularities, and broader societal sensitivities. A globally uniform approach to content moderation is therefore unlikely to achieve a fair and proportionate balance of interests. Thus, it appears necessary to introduce provisions requiring platform providers to adopt region-specific moderation frameworks. Such frameworks should be developed in close cooperation with public authorities, civil society organizations, and local experts in order to ensure that moderation practices genuinely reflect the cultural and contextual diversity inherent in the exercise of freedom of expression across different societies.¹¹⁴ Researchers around the world are already exploring various approaches to adapting AI tools to specific contexts and to accounting for linguistic and cultural diversity. Examples include techniques such as transfer learning and the development of multilingual models.¹¹⁵ Integrating such solutions would not only contribute to a safer and more equitable online environment that strengthens the protection of human rights but could also prove beneficial for platform providers themselves. By improving their capacity to manage online speech through tools capable of capturing contextual nuance and that are combined with well-trained human moderators, platforms can foster more informed moderation decisions that balance the competing fundamental rights effectively.¹¹⁶

¹¹⁴ Politics and Rights Review, *Localized Content Moderation: A Human Rights Approach*, 25 October 2024, <https://politicsrights.com/content-moderation-a-human-rights-approach/>, 28 January 2026.

¹¹⁵ Gavi, *op. cit.* note 102.

¹¹⁶ *Localized Content Moderation: A Human Rights Approach*, *op. cit.* note 114.

If content moderation were designed primarily to protect the rights of users rather than to advance the economic interests of platform providers, a greater reliance on AI-driven moderation might eventually become both feasible and proportionate. Until such conditions are met, however, it remains essential for the EU legislator to establish clearer substantive rules governing the use of these tools, particularly in situations where a balancing of competing fundamental rights is required.

More important than ever, in my view, is that the EU legislator clearly determines the values it seeks to uphold. Rather than yielding to shifting political pressures, it should continue to promote and safeguard its foundational commitments: a Union in which freedom of expression can coexist with other fundamental rights, and in which any restriction of those rights must be necessary, appropriate, and above all proportionate.

REFERENCES

BOOKS AND ARTICLES

1. Al-Zaman, S. M., *Patterns and Trends of Global Social Media Censorship: Insights from 76 Countries*, Sage Journals, volume 87, 10/2024, pp. 1 - 26.
2. Botero Arcila, B.; Griffin, R., *Social Media Platforms and Challenges for Democracy, Rule of Law, and Fundamental Rights*, Study requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, April 2023.
3. Fasel, M.; Weerts, S., *Can Facebook's Community Standards Keep up with Legal Certainty? Content Moderation Governance under the Pressure of the Digital Services Act*, Policy & Internet, volume 16, 2024, pp. 588 - 603.
4. Frosio, G.; Geiger, C., *Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime*, European Law Journal, volume 29, 11/2023, pp. 31 - 77.
5. Gavi, K., *Ethical Challenges in AI-Powered Hate Speech Detection: Balancing Automated Moderation and Dataset Creation*, January 2025.
6. Geiger, C.; Frosio, G.; Izyumenko, E., *Intermediary Liability and Fundamental Rights*, SSRN Electronic Journal, 06/2019.
7. Golunova, V.; Tas, S., *Guardians of Digital Rights: Exploring Strategic Litigation on Data Protection and Content Moderation in the EU*, Nordic Journal of European Law, volume 7, 01/2025, pp. 49 - 66.
8. Güler, M. A., *The Concept of the Welfare State and Typologies of Welfare Regimes: A Review*, Problemy Polityki Społecznej, volume 47, 4/2019, pp. 113 - 130.

9. Hakami, A.; Tazel, R., *The Ethics of AI in Content Moderation: Balancing Privacy, Free Speech, and Algorithmic Control*, ResearchGate, 10/2024.
10. Hesselink, M. W., *The Values Underlying the Draft Common Frame of Reference: What Role for Fairness and "Social Justice"?*, Study No. PE 408.312, European Parliament, Directorate General Internal Policies of the Union, 2008.
11. Husovec, M., *Principles of the Digital Services Act*, Oxford University Press, Oxford 2024.
12. Jodanović, A., *The Digital Services Act Package: Protection of the Fundamental Rights of Digital Service Users in the European Union*, *Regional Law Review*, volume 5, 11/2024, pp. 43 - 61.
13. Mak, C., *Fundamental Rights in European Contract Law: A Comparison of the Impact of Fundamental Rights on Contractual Relationships in Germany, the Netherlands, Italy and England*, Kluwer Law International, Alphen aan den Rijn 2007.
14. Mak, V., *Redefining Equality in European Contract Law: Protecting Consumer Interests in a Post-Consumer Society*, *European Law Open*, 2024, pp. 561 - 586.
15. Mast, T.; Ollig, C., *The Lazy Legislature: Incorporating and Horizontalising the Charter of Fundamental Rights through Secondary Union Law*, *European Constitutional Law Review*, volume 19, 09/2023, pp. 462 - 486.
16. Nishant, R.; Schneckenberg, D.; Ravishankar, M. N., *The Formal Rationality of Artificial Intelligence-Based Algorithms and the Problem of Bias*, *Journal of Information Technology*, volume 39, 1/2024, pp. 19 - 40.
17. Palumbo, A., *Disentangling the Horizontalisation of Fundamental Rights in the Digital Services Act: What Obligations for Online Intermediaries?*, *Rivista di diritto dei media*, volume 2, 10/2024, pp. 100 - 121.
18. Palumbo, A.; Ducuing, C., *The Blurring of the Public-Private Dichotomy in Risk-Based EU Digital Regulation: Challenges for the Rule of Law*, *SSRN Electronic Journal*, 08/2025.
19. Pöschl, M., *Neuvermessung der Meinungsfreiheit*, in: H. Koziol (ed.), *Tatsachenmitteilungen und Werturteile: Freiheit und Verantwortung*, Jan Sramek Verlag, Vienna 2018, pp. 31 - 58.
20. Quintais, P. J.; Appelman, N.; Ó Fathaigh, R., *Using Terms and Conditions to Apply Fundamental Rights to Content Moderation*, *German Law Journal*, volume 24, 11/2023, pp. 881 - 911.
21. Ruschemeier, H.; Quintais, J. P., *Fundamental Rights in Out-of-Court Dispute Settlement under the Digital Services Act*, 2025.
22. Schulz, W.; Ollig, C., *Hybrid Speech Governance: New Approaches to Govern Social Media Platforms under the European Digital Services Act?*,

- Journal of Intellectual Property, Information Technology and E-Commerce Law, volume 14, 02/2024, pp. 560 - 579.
23. Tedoradze, I., *The Principle of Freedom of Contract, Pre-Contractual Obligations Legal Review English, EU and US Law*, European Scientific Journal, volume 13, 02/2017, pp. 62 - 71.
 24. Teubner, G.; Golia, A. Jr., *Societal Constitutionalism in the Digital World: An Introduction*, MPIL Research Paper Series No. 2023-11, 2023.
 25. Vargas Penagos, E., *Platforms on the Hook? EU and Human Rights Requirements for Human Involvement in Content Moderation*, Cambridge Forum on AI: Law and Governance, volume 1, 2025, e23, pp. 1 - 27.
 26. Wendel, M., *Taking or Escaping Legislative Responsibility? EU Fundamental Rights and Content Regulation under the DSA*, in: Ungern-Sternberg, A. et al. (eds.), *Content Regulation in the European Union: The Digital Services Act*, Institut für Recht und Digitalisierung, Trier 2023, pp. 59 - 84.
 27. Wilman, F.; Kalèda, L. S.; Loewenthal, P., *The EU Digital Services Act*, Oxford University Press, Oxford 2024.
 28. Wimmers, J., *The Out-of-Court Dispute Settlement Mechanism in the Digital Services Act: A Disservice to Its Own Goals*, Journal of Intellectual Property, Information Technology and E-Commerce Law, volume 12, 02/2022, pp. 381 - 401.

LEGAL RULES

1. Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012.
2. Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Rome, 4 November 1950.
3. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), OJ L 277, 27 October 2022.

COURT PRACTICE

1. Case C-136/04, *Deutsches Milch-Kontor GmbH v. Germany*, ECR I-10095, 6 October 2005.
2. Case C-162/97, *Nilsson and Others*, ECR I-7477, 19 November 1998.
3. Case C-308/97, *Manfredi*, ECR I-7685, 25 June 1998.

4. Joined Cases C-569/16 and C-570/16, *Stadt Wuppertal v. Bauer and Willmeroth v. Broßonn*, EU:C:2018:871, 6 November 2018.
5. *Sanchez v. France* (GC), App. no. 45581/15, ECtHR, 15 May 2023.

NETWORK RESOURCES

1. Council of Europe, *Freedom of Expression*, The European Convention on Human Rights, <https://www.coe.int/en/web/human-rights-convention/expression>, accessed 26 November 2025.
2. Council of Europe, *Freedom of Expression*, ECHR Toolkit, <https://www.coe.int/en/web/echr-toolkit/la-liberte-dexpression>, accessed 16 February 2026.
3. European Center for Not-for-Profit Law (ECNL), *Algorithmic Gatekeepers: The Human Rights Impacts of LLM Content Moderation - Executive Summary*, 2025, https://ecn1.org/sites/default/files/2025-04/ECNL_LLM_CM_Executive%20Summary_2025.pdf, accessed 4 February 2026.
4. European Commission, *The Digital Services Act, Shaping Europe's Digital Future*, October 2022, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>, 28 October 2025.
5. Griffin, R., *Algorithmic Content Moderation Brings New Opportunities and Risks*, October 2023, <https://www.cigionline.org/articles/algorithmic-content-moderation-brings-new-opportunities-and-risks/>, accessed 04 November 2025.
6. Hendrix, J., *AI Snake Oil: Separating Hype from Reality*, Tech Policy Press, 29 September 2024, <https://www.techpolicy.press/ai-snake-oil-separating-hype-from-reality/>, accessed 30 January 2026.
7. Kayyali, D., *An Advocate's Guide to Automated Content Moderation*, Tech Policy Press, 12 February 2025, <https://techpolicy.press/an-advocates-guide-to-automated-content-moderation/>, accessed 10 February 2026.
8. Politics and Rights Review, *Localized Content Moderation: A Human Rights Approach*, 25 October 2024, <https://politicsrights.com/content-moderation-a-human-rights-approach/>, accessed 28 January 2026.
9. Senfleben, M., *Human Rights Outsourcing and Reliance on User Activism in the DSA*, February 2024, <https://verfassungsblog.de/human-rights-outsourcing-and-reliance-on-user-activism-in-the-dsa/>, accessed 31 December 2025.
10. Țucă, M., *Digital Services Act: Is Article 14(4) Protecting Free Speech or Just Window Dressing?*, January 2025, <https://www.conformia-hub.eu/blog/dsa-art14-free-speech>, accessed 15 January 2026.

UDK: 004.738.5 : 007
004.738.5 : 316.77
34 : 004.8 (4-67 EU)(094.5)
Preliminary communication

Julia Małgorzata Kalus, PhD student

Department of Innovation and Digitalisation in Law, University of Vienna, Austria

E-mail: julia.malgorzata.kalus@univie.ac.at

ORCID: 0009-0008-9326-3999

DEEPFAKE - A PROBLEM ITSELF OR A SYMPTOM OF A DEEPER PROBLEM?

ABSTRACT

The paper tackles one of the most pressing issues regarding social media governance, namely, deep fakes and the spread of disinformation on social media platforms. First, the paper presents deepfakes in a broader perspective of synthetic content and aims to answer the question of whether deepfakes themselves are the problem or rather a symptom of a much more complex issue that lies at the root of the business model of social media platforms and the way they are governed. Additionally, the paper focuses on the threats that deepfakes pose to democracy. Secondly, the paper aims to outline the current regulatory framework dealing with deepfakes and disinformation, and it also touches upon the recently published Code of Practice on marking and labelling of AI-generated content. It critically examines the Code and its possible limitations. Lastly, the paper considers how the approach of public interest technology could be used as a possible theoretical framework to reframe the narrative on deepfake regulation.

Keywords: deepfakes, platform governance, social media platforms, EU law, disinformation, Digital Services Act, Artificial Intelligence Act, transparency

1. INTRODUCTION

1.1. Problem statement

The topic of deepfakes has been present in public debate and academic discourse for a couple of years. Some academics started to underline positive aspects of this technology and even claimed that some of the concerns around deepfakes are exaggerated.¹ Nonetheless, some studies conducted in the past years suggest that

¹ Rauchfleisch, A.; Vogler, D.; de Seta, G., *Deepfakes or Synthetic Media? The Effect of Euphemisms for Labeling Technology on Risk and Benefit Perceptions*, Social Media and Society, volume 11, 09/2025, p. 3.

deepfakes indeed can contribute to the amplification of disinformation.² This is connected not only to their potential to deceive but also to the fact that they negatively influence public trust in media and institutions.³ At the same time, European Union (EU) legislation addressing deepfakes on online platforms has introduced mechanisms such as transparency obligations and risk assessments, which either give platforms a wide discretion in defining their own compliance or which are not addressed to platforms. This paper argues that this approach to deepfake regulation might be insufficient, considering the threats posed by them.

1.2. Research question and contribution

This paper aims to present the concept of deepfake disinformation in a broader context, not focusing on this phenomenon as a content problem that can be addressed through labelling obligation, but rather as an infrastructure problem, rooted in platforms' design. The central research question of this paper is to what extent the current EU legal framework addresses the topic of deepfakes through regulating content. In doing so, the paper aims to contribute to the current legal and policy scholarship on deepfakes and social media platforms by adopting the angle that goes beyond treating deepfakes as just a form of disinformation, and towards the structural role of platform design and recommender systems.

1.3. Outline of the paper

The structure of the paper is the following. The first section of the paper includes research questions, an outline, and the methodology used to develop the paper. In the second section, the paper defines deepfakes and presents them in a broader context of synthetic media. This section provides a definition of a deepfake and provides illustrative examples. Additionally, the section discusses threats that deepfakes pose to democracy, as well as presents deepfakes as a form of disinformation. The third section of the paper focuses on legal analysis. The section starts with a brief introduction of the legal frameworks and then discusses and critically examines each of them. Firstly, the Artificial Intelligence Act (AIA)⁴

² Weikmann, T.; Egelhofer, J.; Lecheler, S, *Beyond Credibility: The Effects of Different Forms of Visual Disinformation*, Journalism & Mass Communication Quarterly, volume 102, 12/2025, p. 1035.

³ Pawelec, M., *Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions*, Digital Society, volume 19, 1/2022, p. 18.

⁴ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down

is analysed together with the first draft of the Code of Practice on marking and labelling of AI-generated content (Code of practice on marking and labelling).⁵ Secondly, the Digital Services Act (DSA),⁶ together with the 2022 Strengthened Code of Practice on Disinformation, which has transitioned into the Code of Conduct on Disinformation (Code of Conduct)⁷ is addressed. Each of the legal instruments is assessed against the problems identified in the second section and presents limitations of an approach that targets content without addressing the underlying problems in the infrastructure. Lastly, the fourth section of the paper concludes the discussion and considers how the public interest technology theory could be applied to the existing legal framework to strengthen the focus on public interest in social media regulation.

1.4. Methodology

The paper adopts an interdisciplinary approach, combining legal primary sources with sources stemming from communication science, psychology, political science, and media studies. Nonetheless, the primary method used in the paper is a legal doctrinal analysis. Legal doctrinal analysis is used to examine the normative content and structure of the European Union secondary law, precisely the AIA and the DSA, as well as soft law instruments adopted as part of these legal frameworks, namely the recently published first draft of the Code of Practice on the marking and labelling of AI-generated content and the Code of Conduct on Disinformation. These instruments were selected as they represent the EU's primary regulatory tools for addressing AI-generated disinformation. The paper analysed these legal instruments in two ways: systematically, by situating them within the broader EU digital regulatory framework, and teleologically, by reading their provisions considering their stated objectives. The EU legislation was accessed through the official EUR-Lex database, and the soft law was accessed through the official website of the European Commission. Additionally, the paper

harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU)No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L, 2024/1689 (hereinafter: AIA).

⁵ European Commission, First Draft Code of Practice on Transparency of AI-Generated Content, February 2026, <https://digital-strategy.ec.europa.eu/en/library/first-draft-code-practice-transparency-ai-generated-content>, 1 March, 2026.

⁶ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277/1 (hereinafter: DSA).

⁷ European Commission, The Code of Conduct on Disinformation, February 2026, p. 1, 2025 <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation>, 26 February, 2026.

is based on the latest state of the art in legal scholarship. Academic legal literature on the matter was identified based on well-established legal databases such as, JIPITEC, Verfassungsblog, Tech Policy Press, HeinOnline, Sage Journals, Cambridge Core, as well as by using Google Scholar.

Before the legal analysis, the paper builds on scholarship from communication science, political science, psychology, and media studies (section 2 of the paper) to establish the empirical and conceptual foundation of the research question. The author identified relevant academic literature in these fields by using databases such as Spring Nature, Sage Journals, SSRN, IEEE Xplore, Taylor Francis Online, and Google Scholar. The identified literature serves two purposes. First, to identify the threats deepfakes pose to democratic discourse and electoral integrity and their capacity to discourage political participation. Secondly, to argue that deepfakes can be understood as a form of disinformation, which explains the inclusion of the Code of Conduct on Disinformation among the instruments under analysis.

2. DEEPFAKES, DEMOCRACY AND DISINFORMATION

2.1. Deepfakes: definition and characteristics

According to the AIA, a deepfake is an "AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful".⁸ The adjective "deep" is used in the definition because this form of content is often created with the use of deep learning.⁹ Deepfakes are part of a broader category of synthetic media,¹⁰ which also encompasses media such as augmented reality, humanoid robots,¹¹ or virtual influencers.¹² While a comprehensive analysis of synthetic media and its nuances is beyond the scope of this paper,¹³ it may briefly be defined as content produced through the application of Artificial Intelligence (AI) technologies.¹⁴

⁸ Art. 3(60) AIA.

⁹ Tolosana, R. *et al.*, *Deepfakes and beyond: A Survey of face manipulation and fake detection*, Information Fusion, volume 64, 12/2020, p. 131.

¹⁰ Van der Sloot, B.; Wagenveld, Y., *Deepfakes: regulatory challenges for the synthetic society*, Computer Law and Security Review, volume 46, 9/2022, p. 1-2.

¹¹ Van der Sloot, B., *Regulating the Synthetic Society*, Hart Publishing, Oxford 2024, p. 14.

¹² Kalpokas, I., *Problematising reality: the promises and perils of synthetic media*, SN Soc Sci, volume 1, 11/2020, p. 1-2.

¹³ See: Millièrè, R., *Deep Learning and Synthetic Media*, Synthese, volume 200, 5/2022.

¹⁴ Kalpokas, I., *op. cit.* note 12, p. 1-2.

Deepfakes are no longer only a domain of technically skilled actors, as the tools necessary for their creation have become progressively more accessible and user-friendly.¹⁵ One of the examples of such tools is the DeepFaceLab, which can be used for face swaps and is available as an open-source software for Windows and macOS.¹⁶ The ease and speed connected to the creation and dissemination of deepfakes are what make them a dangerous tool. This is because tools that do not require programming expertise have made production accessible to virtually anyone, and a deepfake can reach millions of online users through algorithmic amplification before any correction is issued.¹⁷ Deepfakes are considered to be very persuasive mainly because of the use of AI in their production, and in particular, a technique called a generative adversarial network.¹⁸

In the next section, the focus is on the negative impact of deepfakes on democracy, and attention is given to political disinformation. However, it must be acknowledged that 90% of deepfakes present online are a form of violence against women.¹⁹ This form of non-consensual pornographic content also has an indirect impact on democracy as it discourages women from participation in public life.²⁰ One of the recent examples of such a malicious use of deepfake technology is the recent scandal in which German television presenter Collien Fernandes became a victim of a deepfake campaign orchestrated by her husband.²¹ Nonetheless, this paper will not focus specifically on this form of deepfakes since a separate legal framework is considered for this form of deepfakes, as recently, deepfake pornography has gotten attention from the European Parliament (EP). The EP announced that it will call for stronger enforcement of EU law to combat the use

¹⁵ Labuz, M., *A Teleological Interpretation of the Definition of Deep Fakes in the EU Artificial Intelligence Act—A Purpose-Based Approach to Potential Problems With the Word "Existing"*, Policy and Internet, volume 17, 1/2025 p. 2.

¹⁶ DeepFaceLab, How DeepFaceLab Works, <https://deepfacelab.org/#choose>, 31 March 2026.

¹⁷ Momeni, M., *Artificial Intelligence and Political Deepfakes: Shaping Citizen Perceptions Through Misinformation*, Journal of Creative Communications, volume 20, 10/2024, p. 47.

¹⁸ Nieweglowska, M.; Stellato, C.; Sloman, S. A., *Deepfakes: Vehicles for Radicalization, Not Persuasion*, Current Directions in Psychological Science, volume 32, 3/2023, p. 237.

¹⁹ Kira, B., *Deepfakes, The Weaponisation of AI Against Women and Possible Solutions*, Verfassungsblog, June 2024, <https://verfassungsblog.de/deepfakes-ncid-ai-regulation/>, 12 February, 2026.

²⁰ Shukla, V., *Deepfakes and Elections: The Risk to Women's Political Participation*, TechPolicy Press, February 2024, <https://www.techpolicy.press/deepfakes-and-elections-the-risk-to-womens-political-participation/>, 20 February, 2026.

²¹ Parker, J.; Völk, K., *How deepfake porn scandal surrounding TV star rocked Germany*, BBC News, 29 March, 2026, <https://www.bbc.com/news/articles/c9v1m4j47e2o>, 31 March, 2026.

of AI tools to create illegal sexual content.²² Therefore, this malicious use of deepfakes falls outside the scope of this paper. Nonetheless, the author wanted to acknowledge this malicious form of deepfakes.

2.2. Threats posed by deepfakes to democracy

Trust is an essential element required for the effective functioning of democratic processes.²³ If a shared perception of reality is lacking, it is extremely difficult to tackle national and global problems, such as the financial crisis or the rule of law crisis.²⁴ Deepfakes lead to citizens questioning whether what they see is "true", which consequently contributes to a decay of trust in shared facts and truths.²⁵ Therefore, they significantly contribute to the rise of a so-called post-truth society, where it is impossible to distinguish between facts and opinions.²⁶ Some might argue that the spread of half-truths in the digital sphere is not a novelty,²⁷ but the high quality of the content generated by deepfake technology makes it an unprecedentedly dangerous tool.²⁸ It must be pointed out that deepfakes contribute to citizens losing trust not only in democratic processes, such as elections, but also in each other.²⁹ This phenomenon can be described as a 'societal trust decay'.³⁰ As a result of a loss of trust in each other, individuals might feel discouraged from participating in democratic processes.³¹

Deepfakes can change attitudes towards politicians and evoke strong emotions.³² One of the examples of a deepfake that was met with a strong reaction from the

²² European Parliament, Tackling AI deepfakes and sexual exploitation on social media (EP) Briefing, European Parliament, 15 January, 2026, <https://www.europarl.europa.eu/news/en/agenda/plenary-news/2026-01-19/8/tackling-ai-deepfakes-and-sexual-exploitation-on-social-media>, 15 February, 2026.

²³ Chesney, R.; Danielle, C., *Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?* Lawfare, February 2018, <https://www.lawfaremedia.org/article/deepfakes-looming-crisis-national-security-democracy-and-privacy>, accessed 26 February, 2026.

²⁴ *Ibid.*

²⁵ Pawelec, M., *op. cit.* note 3, p. 4.

²⁶ Chesney, R.; Citron, D., *Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics*, Foreign Affairs, volume 98, 2/2019, p. 155.

²⁷ Barber, A., *Freedom of expression meets deepfakes*, Synthese, volume 202, 7/2023, p. 14.

²⁸ *Ibid.*

²⁹ Pawelec, M., *op. cit.* note 3, p. 12.

³⁰ *Ibid.*, p. 19.

³¹ *Ibid.*, p. 18.

³² Dobber, Tom *et al.*, *Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?*, The International Journal of Press/Politics, volume 26, 1/2021, p. 70.

public is a video in which Ukrainian President Volodymyr Zelensky was encouraging Ukrainians to surrender.³³ This is an example of a malicious deepfake manipulation, as it could alter public perception of Ukraine's commitment to defeating Russia's aggression and consequently negatively affect European security. In the current Iranian war, deepfakes are being used as pro-war propaganda. Social media researchers identified a wave of deepfakes on online platforms, in particular on TikTok, portraying women in military uniforms saying "Habibi, come to Iran".³⁴ These deepfakes were spread on social media platforms through fake accounts. Even though deepfakes in question were a clear example of disinformation, as women are not allowed to serve in the Iranian army, deepfakes got a lot of reactions and positive comments, such as "yes".³⁵ This example of a deepfakes campaign shows how deepfakes can reach users and gather their reaction through the use of fake social media accounts led by fake influencers³⁶, and it shows how social media infrastructure can be used to spread disinformation.

2.3. Deepfakes as a disinformation tool

The previous sub-section briefly presented threats that deepfakes pose to democratic societies. Even though it has not yet been measured whether a particular deepfake had an impact on the change of a person's political views, and it is doubtful whether such a measurement would even be possible, it has been established that deepfakes contribute to the amplification of disinformation. This section will consider whether deepfakes fulfil the definition of disinformation.

One of the first definitions of disinformation in European Law appeared in the 2018 version of the Code of Practice on Disinformation.³⁷ Based on definitions of disinformation in the EU law, including 2018 Code of Practice on Disinformation,

³³ Twomey, J. J.; Linehan, C.; Murphy, G., Deepfakes in warfare: new concerns emerge from their use around the Russian invasion of Ukraine, *The Conversation*, October 2023, 2023, <https://theconversation.com/deepfakes-in-warfare-new-concerns-emerge-from-their-use-around-the-russian-invasion-of-ukraine-216393>, 31 March, 2026.

³⁴ Marco Silva, Flood of AI soldiers push pro-Iran messages during war, *BBC News*, 12 March 2026, <https://www.bbc.com/news/videos/cy9gw900dp9o>, 1 April, 2026.

³⁵ Berger, E., 'They feel true': political deepfakes are growing in influence – even if people know they aren't real, *The Guardian*, 28 March, 2026, <https://www.theguardian.com/technology/2026/mar/28/military-deepfakes-ai-propaganda-money>, 1 April 2026.

³⁶ *Ibid.*

³⁷ Bleyer-Simon, K.; Reviglio, U., Defining Disinformation across EU and VLOP Policies, *European Digital Media Observatory*, October 2024, p.11, <https://edmo.eu/wp-content/uploads/2024/10/EDMO-Report-%E2%80%93-Defining-Disinformation-across-EU-and-VLOP-Policies.pdf>, 1 April, 2026.

it is possible to distinguish key elements that need to be fulfilled for a content to be considered disinformation: (i) content must be verifiably false or misleading, (ii) it must have the potential to cause harm to society, (iii) it is spread intentionally (iv) possibly for economic or political gain.³⁸ When it comes to deepfakes, the first element is fulfilled as at the core of the deepfake definition lies the fact that they falsely resemble reality, and are therefore misleading. Considering the discussion in the previous section, in which potential risks of deepfakes to democracy and internal security were presented, the second element is also fulfilled. The last element relating to political and economic gain seems to also be fulfilled, as in most cases, political deepfakes are spread to serve a specific political agenda.³⁹

Some scholars argue that deepfakes are not a new threat and that they rather belong to the broader disinformation landscape.⁴⁰ At the same time, it is debatable whether deepfakes alone could actually contribute to the spread of disinformation. Some studies suggest that, to be successful, deepfake campaigns would need to be precisely targeted,⁴¹ which strongly links their success in disinformation to social media infrastructure,⁴² and fake social media accounts, bots, and recommender systems.⁴³

Additionally, studies conducted in the past years confirm that algorithms on social media platforms contribute to the spread of emotionally charged content.⁴⁴ One study, which focused on platforms such as TikTok, Instagram and Facebook, showed that the negative and emotionally charged content around port security in Split was prioritised by algorithms on these platforms.⁴⁵ Additionally, the study

³⁸ *Ibid.*, p. 3.

³⁹ Szabo, L.V.; Bader, S., *Deepfake content in political communication*, Convergence: The International Journal of Research into New Media Technologies, volume 0, 2026, p. 10.

⁴⁰ Łabuz, M.; Nehring, C., *On the way to deep fake democracy? Deep fakes in election campaigns in 2023*, year 2024, 23:454–473 *European Political Science*, volume 23, 12/2024, p. 465.

⁴¹ Fathaigh, R. et.al., *Microtargeted propaganda by foreign actors: An interdisciplinary exploration*, Maastricht Journal of European and Comparative Law, volume 28, 11/ 2021, Vol. 28(6) 2021, p. 866.

⁴² Birrer, A.; Just, N., *What We Know and Don't Know about Deepfakes: An Investigation into the State of the Research and Regulatory*, New Media and Society, volume 27, 12/2025, p. 6828.

⁴³ Von Sikorski, Ch.; Hameleers, M., *Disinformation in the Age of Artificial Intelligence (AI): Implications for Journalism and Mass Communication*, Journalism & Mass Communication Quarterly, volume 102, 11/2025, p. 944.

⁴⁴ See: Gombar, M.; M. Boban, *Research on the Impact of Algorithmic Echo Chambers on Perceptions and Attitudes of Social Network Users in a Digital Society*, MIPRO 48th ICT and Electronics Convention, Opatija, Croatia, June 2025, <https://ieeexplore.ieee.org/document/11131918>, 1 April, 2026.

⁴⁵ *Ibid.*, p. 1028-1029.

showed that algorithms are not a neutral technology, but have an active role in spreading disinformation.⁴⁶ The results of the study are one of the testimonies that the discussion on deepfake disinformation should not be focused only on addressing the content, but rather the overall infrastructure for its spread.

3. REGULATORY FRAMEWORK

In the last section, the topic of deepfakes has been framed as a symptom of a disease rather than an illness. It was argued that even though deepfakes are a sophisticated method of disinformation, and their effects can be very harmful for public trust in democratic societies, the problem seems to lie in the channels that focus on distributing this form of content.

This section will deal with the analysis of the EU Law that addresses deepfakes and content on social media platforms. First, the AIA will be analysed, and specifically, Article 50(4) of the AIA will be addressed, as well as the Code of Practice on marking and labelling of AI-generated content. The next sub-section will focus on the DSA, which is a crucial puzzle in the regulatory landscape regarding deepfakes, as they are mainly spread on major technological platforms.⁴⁷

3.1. The Artificial Intelligence Act

The AIA includes the first explicit definition of a deepfake in European Law.⁴⁸ Additionally, Article 50 of the AIA imposes a transparency obligation on deployers of AI systems capable of producing deepfakes. It is worth noting that the AIA is a market-focused legislation, meaning that it primarily regulates the process of developing and bringing AI systems to the market,⁴⁹ and was designed as a product safety regulation.⁵⁰ Therefore, even though ensuring a high level of protection of democracy is mentioned in the scope of this legislation,⁵¹ it is not its main objective. Additionally, the AIA does not focus on disinformation explicitly in its provisions. At the same time, the EU legislator has acknowledged the potentially

⁴⁶ *Ibid.*, p. 1032.

⁴⁷ Soundarya, B.; Gururaj, H. L., *Deepfake detection: critical review of state-of-the-art approaches and future perspectives*, Discover Applied Sciences, volume 8, 1/2026, p. 20.

⁴⁸ See: Art. 3(60) AIA.

⁴⁹ Almada, M.; Petit, N., *The EU AI Act: Between the Rock of Product Safety and the Hard Place of*

Fundamental Rights, Common Market Law Review, volume 62, 2/2025, p. 104.

⁵⁰ Art. 1(1) AIA.

⁵¹ *Ibid.*

harmful effects of synthetic content on the information landscape and public knowledge.⁵² Further, Recital 134 explicitly addresses deepfakes and underlines the importance of transparency and labelling of deepfake content.⁵³

3.1.1. Actors in the AIA

To understand the transparency obligations in the AIA that apply to AI-generated content, including deepfakes, it is necessary to explain the main actors in this legislation. The AIA applies to providers and deployers of AI systems. Both are any natural and legal persons, or other bodies such as public authorities.⁵⁴ A provider of an AI system is an actor that develops an AI system or a general-purpose AI model and places it on the market,⁵⁵ whereas a deployer uses it under its authority, unless it is in the course of a personal activity.⁵⁶

In the context of deepfakes, providers of AI systems would usually be companies that develop AI systems that can be used to produce deepfakes, such as the previously mentioned DeepFaceLab. Deployers of AI systems are actors that use the AI system, in this case, natural persons creating deepfakes. What raises enforcement concerns is the general exemption to the scope of the AIA in Article 2(10), which states that the regulation does not apply to persons who use AI systems in a purely private capacity.⁵⁷ It is claimed that since deepfakes are mostly created with the intent to be published publicly, this exception should not be applicable.⁵⁸ Therefore, a person creating a deepfake would be considered a deployer, and the provisions of the AIA should apply to a deepfake creator.⁵⁹ This interpretation is reasonable and would be preferred in order to ensure compliance with transparency obligations. Nonetheless, it is difficult to assess what exactly qualifies as a "personal activity" and it could potentially lead to overreliance on this exemption,⁶⁰ and consequently limit adherence to transparency obligations.

⁵² Recital 133 AIA.

⁵³ Periello, L.E., *Blurred realities: Legal strategies for the deepfake era*, Maastricht Journal of European and Comparative Law, volume 0, 3/2026. p. 15.

⁵⁴ Arts. 3(3),3(4) AIA

⁵⁵ Art. 3(3) AIA.

⁵⁶ Article 3(4) AIA.

⁵⁷ Periello, L.E., *op. cit.* note 54, p. 25.

⁵⁸ *Ibid.*

⁵⁹ *Ibid.*

⁶⁰ *Ibid.*

3.1.2. Do deepfakes qualify as high-risk?

The AIA adopts a risk-based approach and qualifies AI systems into categories based on the level of risk they pose to fundamental rights and safety of individuals.⁶¹ An AI system can be classified as a minimal risk,⁶² limited risk,⁶³ high-risk,⁶⁴ or unacceptable risk (prohibited).⁶⁵ Depending on the risk level, the AIA assigns different obligations to providers and deployers.

When it comes to high-risk AI systems, Article 6(2) of the AIA states that AI systems can be qualified as high-risk if they are included in Annex III. In the context of political disinformation, it can be observed that point 8 in Annex III seems to be the most relevant, as it refers to "administration of justice and democratic processes".⁶⁶ However, it applies explicitly to AI systems that have the potential to influence the outcome of elections or a referendum.⁶⁷ Therefore, it could be understood that this provision relates to AI systems that are directly used in voting systems, such as systems used for vote counting or systems used in the assistance with the voting procedure.⁶⁸ Additionally, recital 62, read in conjunction with Article 6 AIA and point 8(b) of Annex III AIA, specifies that it relates to the right to vote as per Article 39 of the EU Charter of Fundamental Rights. Therefore, it can be stated that this provision does not apply to AI systems used for the purpose of political disinformation.⁶⁹ As analysed in section two of this paper, there are diverging outcomes of studies on whether deepfakes are a successful disinformation tool. Consequently, considering recital 62, it can be stated that AI systems used to generate political disinformation do not qualify as high-risk. However, if they are used to directly infringe on the person's right to vote, obligations for high-risk AI systems would apply. Therefore, even though the AIA includes provisions of high-risk AI systems, it is not clear whether they would apply to the AI systems used to spread disinformation or content that qualifies as disinformation.

⁶¹ Gasser, U.; Palfrey, J., *Advanced introduction to Law and Digital Technologies*, Elgar Advanced Introductions, 2025, p. 58.

⁶² Ebers, M., *Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act*, European Journal of Risk Regulation, volume 16, 9/2025, p. 687.

⁶³ Recital 132 AIA.

⁶⁴ Art.6 AIA.

⁶⁵ Art. 5 AIA.

⁶⁶ Krack, N.; Dutkiewicz, L.; De Meyere, J., *Generative Artificial Intelligence and Disinformation*, in Ginsborg, L.; Gori, P. (eds), *Disinformation: A Multi-Disciplinary Analysis*, Springer Nature, Switzerland 2026, p. 275

⁶⁷ Annex III Point 8 AIA

⁶⁸ Krack, N., Dutkiewicz, L. De Meyere, J., *op. cit.* note 65, p. 276.

⁶⁹ *Ibid.*

Consequently, AI systems used to generate deepfakes and spread deepfake disinformation would most likely not be classified as high-risk obligations, and the provisions for high-risk AI systems would likely not apply to them. The scope of this provision must be further specified by the case law of the Court of Justice of the European Union.

3.1.3. Transparency obligations for providers and deployers of AI systems generating deepfakes

Another important provision in the AI regarding deepfakes is Article 50, which establishes transparency obligations for certain AI systems. Article 50 imposes obligations on both providers and deployers of AI systems that interact with natural persons or generate synthetic content. Most relevantly for this paper, Article 50(4) requires "deployers of an AI system that generates or manipulates image, audio, or video content constituting a deep fake"⁷⁰ to disclose that the content has been artificially manipulated. This provision does not apply in cases in which authorization has been given by a person presented in images, videos, or audio content, or if it was *inter alia* produced to exercise the freedom of expression or serve as a parody.⁷¹ Even though the inclusion of this provision is a noble development and a step towards a more transparent online environment, the provision remains problematic. Many open-ended questions arise when reading the text of the provision, and there are several critical points that are connected to the discussion in the previous section of deepfakes being a symptom rather than a disease.

First, assessing what qualifies as a legitimate speech and what deepfakes can be regarded as a freedom of expression is problematic. The AIA does not state clearly where the line lies between, for instance, artistic expression and a deepfake that must be labelled.⁷² Lack of clarity on what constitutes a parody or artistic expression could lead to harmful abuses of this exemption.⁷³

Secondly, there is a general concern regarding the enforcement of transparency obligations. The territorial scope of the AIA, included in Article 2(1)(a)(b)(c), covers not only actors based in the EU, but also actors who deploy or provide an AI system whose output reaches the EU. Consequently, deepfakes reaching EU

⁷⁰ Art. 50(4) AIA.

⁷¹ *Ibid.*

⁷² Periello, L.E., *op. cit.* note 54, p. 25.

⁷³ *Ibid.*

citizens must be subjected to transparency obligations.⁷⁴ It means that in theory, the scope of the AIA is extraterritorial. However, tracking individuals who produce and share deepfakes and enforcing the transparency obligation across international borders, especially given the decentralized channels, risks being a Sisyphean task.⁷⁵ In order to provide for effective enforcement, measures such as cross-border mechanisms or international agreements should be in place.⁷⁶ More detailed discussion on the extraterritorial enforcement of the transparency obligations applicable to deepfakes constitutes another research field, which falls outside the scope of this paper.

To conclude, Article 50(4) addresses the symptom, being, for the purpose of this paper, the existence of an AI-generated content that could harm democratic processes, without engaging with the structural problems and issues related to the infrastructure. It is because the regulators decided to include deepfakes as a limited risk category and, therefore, subjected them to mostly transparency obligations.⁷⁷ It must be noted that according to Article 50(6), AIA does not exclude that transparency obligations go hand in hand with high-risk obligations. Therefore, it is not unlikely that in the future some deepfake applications might be considered high-risk as well.⁷⁸

3.1.4. Code of Practice on marking and labelling of AI-generated content

To support the implementation of the obligations in Article 50(4) of the AIA, the AI Office, a body designated by the European Commission that gathers experts on AI,⁷⁹ initiated the process of creating the Code of Practice on marking and labelling of AI-generated content. The aim is to allow providers and deployers to prepare for compliance before the rules take effect in August 2026.⁸⁰ The Code of Practice on marking and labelling finds its legal basis in Article 95 of the AIA. Adherence to the Code of Practice is voluntary, and it is addressed to its signatories.⁸¹ At the time of writing this paper, only the first draft of the Code of Practice published in February 2026 is available. According to the European

⁷⁴ *Ibid.*

⁷⁵ *Ibid.*, p. 27.

⁷⁶ *Ibid.*

⁷⁷ *Ibid.*, p. 23.

⁷⁸ *Ibid.*, p. 22.

⁷⁹ Art. 64(1) AIA.

⁸⁰ European Commission, *op. cit.* note 5.

⁸¹ European Commission, First Draft Code of Practice on Transparency of AI-Generated Content, February 2026, p. 2, <https://digital-strategy.ec.europa.eu/en/library/first-draft-code-practice-transparency-ai-generated-content> 1 March, 2026.

Commission, the second draft of the Code of Practice is foreseen to be published in March 2026.⁸² Therefore, the content of the code discussed in this paper might not be up to date once it is published. Nonetheless, the Code of Practice is still worth examining. The limitations of the code, such as its voluntary nature, show the overall approach of the Commission to the regulation of AI-generated content, which is focused largely on transparency obligations and which lacks clear guidance on enforcement.

The Code on Practice proposes an EU-wide icon that would signal that the content is a deepfake.⁸³ This initiative is a positive development. Nonetheless, it stems from the idea that there is a willingness from deployers of the AI systems for the purpose of deepfake creation to comply with legal obligations. However, the aim of deepfake creators is often to destabilise and spread disinformation.⁸⁴ Therefore, specifications in relation to labelling the content, yet again, do not solve the root of the problem. Additionally, a lot of emphasis in the Code of Practice is placed on AI literacy.⁸⁵ While it is a measure that must go hand in hand with other legal obligations, the burden cannot be solely placed on the individual seeing a deepfake, considering the power imbalance between users of platforms and platform administrators. The DSA aims to mitigate these imbalances, which is why both legislations are jointly analysed in this paper.

3.2. The Digital Services Act (DSA)

The DSA became an enforceable law in February 2024.⁸⁶ The topic of deepfakes is not directly addressed in the legislation, and in contrast to the AIA, the DSA does not include an explicit definition of a deepfake. It is worth mentioning that the DSA does not focus on AI but rather on digital intermediaries.⁸⁷ The legislation distinguishes between Very Large Online Platforms (VLOPS) and Very Large Search Engines (VLSE). Platforms having more than 45 million users per month qualify as VLOPS.⁸⁸ The word 'disinformation' appears in the DSA thirteen times,⁸⁹ but only in the recitals of the regulation, and it does not include an explicit definition of disinformation in its provisions.

⁸² *Ibid.*

⁸³ *Ibid.*, p. 24 (Measure 1.2.2).

⁸⁴ Fathaigh, R. *et.al.*, *op. cit.* note 40, p. 857.

⁸⁵ European Commission, *op. cit.* note 79., p. 21(recital e).

⁸⁶ Art. 93 DSA.

⁸⁷ See: Art. 2(1) DSA.

⁸⁸ Art. 33(1) DSA.

⁸⁹ Recitals 2, 9, 69, 83, 84, 88, 95, 104, 106, 108 DSA.

3.2.1. Risk assessment and risk mitigation

One of the most important obligations of VLOPS is risk assessment, introduced in Article 34 of the DSA. The DSA distinguishes four categories of risks,⁹⁰ such as risks to democratic processes or risks posed by illegal content.⁹¹ The concept of risks is also a crucial element of the AIA.⁹² However, the DSA does not adopt a risk-based approach, but rather introduces a concept of systemic risk.⁹³ The understanding of the concept of systemic risk in the DSA is broad, and it does not include an exhaustive list of risks.⁹⁴ It is the platforms themselves that must identify and analyse them.⁹⁵

Next to the risk assessment, VLOPs are also required to introduce mitigation measures.⁹⁶ The DSA includes various examples of mitigation measures, such as awareness-raising,⁹⁷ or adapting the design of the interfaces.⁹⁸ Notably, the last mitigation measure listed in Article 35 refers to "generated or manipulated image, audio or video that appreciably resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful".⁹⁹ Although deepfakes are not explicitly mentioned in the provision, they clearly fall within its scope, as it indirectly sets out a definition of a deepfake, but without mentioning AI.¹⁰⁰ This proposed mitigation measure requires intermediaries to inform users that the content was manipulated by "prominent markings".¹⁰¹ Therefore, it is similar to Article 50(4) of the AIA. The transparency requirements, such as marking and labelling, might not be the most effective, as according to a recent psychological study, individuals tend to rely on the content of deepfakes even if they are made aware that it is not true or correct.¹⁰²

⁹⁰ Recital 79 DSA.

⁹¹ Art. 34 DSA.

⁹² Krack, N.; Dutkiewicz, L.; De Meyere, J., *op. cit.* note 65, p. 279.

⁹³ Recital 76 DSA.

⁹⁴ *Ibid.*

⁹⁵ Art. 34 (1) DSA

⁹⁶ Art. 35 DSA

⁹⁷ Art. 35(i) DSA.

⁹⁸ Art. 35(k) DSA.

⁹⁹ *Ibid.*

¹⁰⁰ Krack, N.; Dutkiewicz, L.; De Meyere, J., *op. cit.* note 65, p. 278.

¹⁰¹ Art. 35 (k) DSA.

¹⁰² Clark, S.; Lewandowsky, S., *The Continued Influence of AI-Generated Deepfake Videos despite Transparency Warnings*, Communications Psychology, volume 4, 1/2026, p. 10.

3.2.2. Recommender system transparency

So far, this section has focused on the obligations of VLOPs regarding risk assessment and risk mitigation. The DSA also includes an important provision dealing with obligations for recommender systems,¹⁰³ Article 27, which is arguably the most directly relevant provision for this paper's central argument. This Article requires intermediaries to present in their terms and conditions at least one option for a recommender system that does not include profiling, and to make their recommended systems transparent.¹⁰⁴ The DSA acknowledges that recommender systems play an important role in platforms' business models and it defines them as a tool that algorithmically suggests, ranks, and prioritises information and is capable of amplifying certain messages.¹⁰⁵

The option to allow individuals to decide not to have a recommender system based on profiling can be seen as a step towards empowering individuals, a process that is considered to be an important part of fair governance.¹⁰⁶ However, the provision does not prohibit systems that use engagement-maximising recommendations, which is the main mechanism that allows for emotionally engaging content, such as deepfakes, to be spread on social media platforms.¹⁰⁷ Therefore, the provision only focuses on transparency, rather than addressing the core of the problem. Secondly, there are some practical limitations to this provision and enforcement issues exemplified by researchers in non-governmental organisations, such as the EU Disinfo Lab.¹⁰⁸ One investigation conducted by the Dutch NGO, Bits of Freedom,¹⁰⁹ showed that even when users decide to disable profiling on Instagram, some of the features on the application, such as direct messages, become inaccessible.¹¹⁰ This case well exemplifies how big technological companies try to circumvent legal obligations imposed on them. Additionally, it is very unlikely

¹⁰³ Art. 27 DSA.

¹⁰⁴ Art. 27(3) DSA.

¹⁰⁵ Recital 70 DSA.

¹⁰⁶ Gasser U.; Palfrey, J., *Advanced Introduction to Law and Digital Technologies*, Elgar Advanced Introduction 2025, p. 120.

¹⁰⁷ Milli, S. *et al.*, *Engagement, User Satisfaction, and the Amplification of Divisive Content on Social Media*, *PNAS Nexus*, volume 4, 3/2025, p. 4-5.

¹⁰⁸ See: EU Disinfo Lab, About, <https://www.disinfo.eu/about-us/problem/>, 28 February, 2026.

¹⁰⁹ See: Zenger, R.; Austin, E.; Knaap, M., Judge in the Bits of Freedom vs. Meta lawsuit: Meta must respect users' choice, 2 Oktober 2025, <https://www.bitsoffreedom.nl/2025/10/02/judge-in-the-bits-of-freedom-vs-meta-lawsuit-meta-must->, 25 February, 2026.

¹¹⁰ See: Aşmane, K.L.; McNamee, J., Malicious semi-compliance as the platform approach to EU regulation, EU DisinfoLab, 25 November, 2025, <https://www.disinfo.eu/malicious-semi-compliance-as-platform-approach-to-eu-regulation/>, 28 February, 2026.

that an average user will read the provision and disable the profiling features.¹¹¹ The effectiveness of the provision is consequently not only based on the will of users to change the settings but also on how well the platforms inform users about this possibility.¹¹² This issue could be connected to the phenomenon of dark patterns. However, this discussion falls outside of the scope of this paper.

3.2.3. Code of Conduct on Disinformation: Can it be a hope for the future?

The 2022 Code of Practice on Disinformation is a crucial soft law when it comes to EU policy efforts in tackling disinformation. At the start of 2025, the Commission approved incorporating the 2022 Code of Practice, now reformulated as the Code of Conduct on Disinformation, into the DSA framework.¹¹³ The parties adhere to the Code of Conduct voluntarily.¹¹⁴ The transition into the Code of Conduct also strengthens the character of the document, making the commitments of the signatories auditable.¹¹⁵ However, adherence to the Code of Conduct remains voluntary.¹¹⁶ As of 13 February 2025, the Code has forty-two signatories, including major online platforms and search engines like Meta and Google, fact-checkers, and representatives of civil society organisations.¹¹⁷ Notably, online platform X withdrew its signature from the Code of Practice in 2023.¹¹⁸ The voluntary nature of the Code and lack of sanction for its implementation render it a rather insufficient mechanism. Additionally, the current trend of social media platforms, withdrawal from fact-checking practices, with Meta being a primary example,¹¹⁹ is a concerning development. The abolishment of Meta's fact-

¹¹¹ Hakkarainen, J.; Savolainen, L., *Individual choice, collective effects: recommender systems, law by design, and the DSA's double choice architecture*, Information, Communication and Society, volume 0, 12/2025, p. 6-7.

¹¹² *Ibid.*

¹¹³ European Commission, The Code of Conduct on Disinformation, 13 February, 2025, <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation>, 20 February, 2026.

¹¹⁴ *Ibid.*, p. 1.

¹¹⁵ Ginsborg, L.; Gori, P. *Disinformation: a multi-disciplinary analysis*, Springer 2026, p. 557.

¹¹⁶ *Ibid.*

¹¹⁷ *Ibid.*

¹¹⁸ Polona, C., Fact-checking and content moderation, European Parliamentary Research Service, February 2025, p. 2, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769493/EPRS_ATA\(2025\)_12_February_2026](https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769493/EPRS_ATA(2025)_12_February_2026).

¹¹⁹ Körömi, C.; Haec, P; Cheslow, D, Zuck goes full Musk, dumps Facebook fact-checking program 7 January 2025, POLITICO, <https://www.politico.eu/article/mark-zuckerberg-full-elon-musk-dump-facebook-fact-checker/>, 20 February 2026.

checking mechanisms is momentarily limited only to the US.¹²⁰ Last year, Marc Zuckerberg openly called the EU's content moderation practices "censorship".¹²¹ It remains to be seen how Meta will continue complying with EU regulations. The voluntary nature of the Code of Conduct is even more problematic in the current political atmosphere, where companies fail to comply even with binding obligations. Lack of compliance with the DSA by X resulted in a 120 million euro fine, which was issued at the end of 2025.¹²² After the issuance of the fine, the CEO of X called for the abolishment of the EU and expressed his support for anti-democratic EU parties.¹²³ This case shows that platforms lack the willingness to comply with EU law. In these times, it is important that the EU addresses the core of the issue, being the platform's infrastructure.

3.3. Legal framework: Concluding Remarks

Article 50(4) of the AIA, including labelling and marking obligations, as well as the transformation of the 2022 Strengthened Code of Practice on Disinformation into the Code of Conduct in 2025, are needed improvements to the existing legal framework. However, currently, the AIA and the DSA focus mostly on transparency obligations. While DSA addresses the issue of recommender systems, the obligations in Art. 27 are not enforced, and platforms find ways to circumvent them. Additionally, a lot of discretion is left to platforms to identify risks and introduce mitigation measures. Transparency obligations in Article 50 raise challenges in relation to extraterritorial enforcement and application of freedom of expression exemption, as well as the personal use exemption. The official version of the Code of Practice on marking and labelling of AI-generated content, which is expected to be published in summer 2026, could offer more clarity on that. However, in the author's opinion, the code will likely uphold its transparency-focused nature and only address technical aspects of how the labelling should be designed.

¹²⁰ *Ibid.*

¹²¹ Powers, C., Zuckerberg calls on US to defend tech companies against European 'censorship', Euroactiv, 12 January, 2025, <https://www.euractiv.com/news/zuckerberg-calls-on-us-to-defend-tech-companies-against-european-censorship/>, 26 February, 2026.

¹²² European Commission, Commission fines X €120 million under the Digital Services Act, European Commission Press Corner, 5 December 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934, 1 April, 2026.

¹²³ European Digital Rights (EDRI), Press Release: EU stands up to Big Tech with €120 million fine to X, 8 December 2025, EDRI Resources, <https://edri.org/our-work/eu-stands-up-to-big-tech-with-e120-million-fine-to-x/>, 1 April 2026.

4. CONCLUSION: PUBLIC INTEREST TECHNOLOGY AS A WAY FORWARD

The paper argued that deepfakes pose threats to democracy and can be a successful disinformation tool when paired with adequate dissemination tools. It was also analysed that algorithms of social media platforms tend to favour emotionally charged content and therefore amplify the spread of political deepfakes. Section 3 of this paper focused on the analysis of provisions of the AIA and the DSA, together with relevant soft laws, with an aim to address the research question of the paper and assess the extent to which these frameworks address deepfakes solely as a content issue. Based on the doctrinal analysis conducted, it can be stated that these two regulations are mainly focused on transparency obligations. Provisions that aim to address the core of the issue, such as Article 27 of the DSA, do not prohibit the use of algorithms that amplify radical content. In addition, as shown in the investigation of the NGO Bits of Freedom, platforms do not fully comply with this obligation. When it comes to the AIA, AI systems used to create deepfakes are only subject to transparency obligations that raise enforcement concerns.

To reframe the approach to regulating social media platforms and deepfakes, it is important to consider how to organise and better govern informational infrastructure. One of the promising theoretical frameworks that could be used in this context is the concept of public interest technology. Public Interest Technology is both a concept and a field of study, which is rooted in the idea that technology should be developed in the interest of the public, not to serve corporations or politics.¹²⁴ It is strongly connected to the public interest concept, which is one of the main concepts in political and legal theory and dates back to the works of Plato and Aristotle.¹²⁵ Within legal scholarship, public interest was described as a bridge between democratic values and regulation.¹²⁶

Relying on the concept of public interest technology in regulating social media platforms would put the welfare of the public at the centre, rather than the economic interests of platforms, which is currently the case. When it comes to the discussed legal frameworks, using public interest technology could mean

¹²⁴ Carayannis, E. G.; Erokhin, V., *Democracy, Environment, and Technology: The Cases of AI and Fusion Energy* Springer Nature, Switzerland 2025, p. 49.

¹²⁵ Züger, T.; Asghari, H., *AI for the public. How public interest theory shifts the discourse on AI*, AI & SOCIETY volume 38, 4/2023, p. 816.

¹²⁶ *Ibid.*

involving the public in the risk assessment process under Article 34 of the DSA¹²⁷ or prohibiting recommender systems that amplify the spread of emotionally driven content. Another possibility would be to include deepfakes in the category of high-risk AI systems and therefore impose more strict obligations on providers and deployers of AI systems that generate deepfakes. Alternatively, using the public interest technology approach could mean that the personal activity exception in Article 2(1) AIA would be read by courts in a restrictive manner, so it does not cover persons developing deepfakes. Even though limited transparency obligations are not an adequate measure, this would allow for some level of protection to be given to users of online platforms encountering deepfake content.

The development of decentralized platforms is also an idea that is often presented in the academic discourse.¹²⁸ Exploring how the decentralized social media platforms could fit into the European legal system and national laws of member states represents an idea for further research.

REFERENCES

BOOKS AND ARTICLES

1. Almada, M.; Petit, N., *The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights*, Common Market Law Review, volume 62, 2/2025, pp. 85-120.
2. Barber, A., *Freedom of expression meets deepfakes*, Synthese, volume 202, 7/2023, 1-17.
3. Birrer, A.; Just, N., *What We Know and Don't Know about Deepfakes: An Investigation into the State of the Research and Regulatory*, New Media and Society, volume 27, 12/2025, 6819-6838.
4. Carayannis, E. G.; Erokhin, V., *Democracy, Environment, and Technology: The Cases of AI and Fusion Energy* Springer Nature, Switzerland 2025.
5. Chesney, R.; Citron, D., *Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics*, Foreign Affairs, volume 98, 2/2019, 147-155.

¹²⁷ Correia de Carvalho, M., *It will be what we want it to be: Sociotechnical and Contested Systemic Risk at the Core of the EU's Regulation of Platforms' AI Systems*, Journal of Intellectual Property, Information Technology and Electronic Commerce Law, volume 16, 3/2025, p. 38.

¹²⁸ See: Bertelsmann Stiftung, *Decentralized Social Media Platforms as a Path to a More Resilient Information Ecosystem*, January 2026 <https://www.bertelsmann-stiftung.de>, 28 February 2026.

6. Clark, S.; Lewandowsky, S., *The Continued Influence of AI-Generated Deepfake Videos despite Transparency Warnings*, Communications Psychology, volume 4, 1/2026, 1-12.
7. Correia de Carvalho, M., *It will be what we want it to be: Sociotechnical and Contested Systemic Risk at the Core of the EU's Regulation of Platforms' AI Systems*, Journal of Intellectual Property, Information Technology and Electronic Commerce Law, volume 16, 3/2025, 35-72.
8. Dobber, Tom *et al.*, *Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?*, The International Journal of Press/Politics, volume 26, 1/2021, 69-91.
9. Ebers, M., *Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act*, European Journal of Risk Regulation, volume 16, 9/2025, 684–703.
10. Fathaigh, R. *et.al.*, *Microtargeted propaganda by foreign actors: An interdisciplinary exploration*, Maastricht Journal of European and Comparative Law, volume 28, 11/ 2021, Vol. 28(6) 2021, 856- 877.
11. Gasser, U.; Palfrey, J., *Advanced introduction to Law and Digital Technologies*, Elgar Advanced Introductions, 2025.
12. Ginsborg, L.; Gori, P. *Disinformation: a multi-disciplinary analysis*, Springer 2026.
13. Hakkarainen, J.; Savolainen, L., *Individual choice, collective effects: recommender systems, law by design, and the DSA's double choice architecture*, Information, Communication and Society, volume 0, 12/2025, 1-18.
14. Kalpokas, I., *Problematizing reality: the promises and perils of synthetic media*, SN Soc Sci, volume 1, 11/2020, 1-2.
15. Krack, N.; Dutkiewicz, L.; De Meyere, J., *Generative Artificial Intelligence and Disinformation*, in Ginsborg, L.; Gori, P. (eds), *Disinformation: A Multi-Disciplinary Analysis*, Springer Nature, Switzerland 2026.
16. Łabuz, M., *A Teleological Interpretation of the Definition of Deep Fakes in the EU Artificial Intelligence Act—A Purpose-Based Approach to Potential Problems With the Word "Existing"*, Policy and Internet, volume 17, 1/2025, 1-14.
17. Łabuz, M.; Nehring, C., *On the way to deep fake democracy? Deep fakes in election campaigns in 2023*, year 2024, 23:454–473 European Political Science, volume 23, 12/2024, 454–473
18. Milli, S. *et al.*, *Engagement, User Satisfaction, and the Amplification of Divisive Content on Social Media*, PNAS Nexus, volume 4, 3/2025, 1-10.
19. Millièrè, R., *Deep Learning and Synthetic Media*, Synthese, volume 200, 5/2022, 1-27.

20. Momeni, M., *Artificial Intelligence and Political Deepfakes: Shaping Citizen Perceptions Through Misinformation*, Journal of Creative Communications, volume 20, 10/2024, 41-56.
21. Nieweglowska, M.; Stellato, C.; Sloman, S. A., *Deepfakes: Vehicles for Radicalization, Not Persuasion*, Current Directions in Psychological Science, volume 32, 3/2023, 236-241
22. Pawelec, M., *Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions*, Digital Society, volume 19, 1/2022, 1-37.
23. Periello, L.E., *Blurred realities: Legal strategies for the deepfake era*, Maastricht Journal of European and Comparative Law, volume 0, 3/2026, 1-32.
24. Rauchfleisch, A.; Vogler, D.; de Seta, G., *Deepfakes or Synthetic Media? The Effect of Euphemisms for Labeling Technology on Risk and Benefit Perceptions*, Social Media and Society, volume 11, 09/2025, 1-12.
25. Soundarya, B.; Gururaj, H. L., *Deepfake detection: critical review of state-of-the-art approaches and future perspectives*, Discover Applied Sciences, volume 8, 1/2026, 1-32.
26. Szabo, L.V.; Bader, S., *Deepfake content in political communication*, Convergence: The International Journal of Research into New Media Technologies, volume 0, 2026, 1-17.
27. Tolosana, R. et al., *Deepfakes and beyond: A Survey of face manipulation and fake detection*, Information Fusion, volume 64, 12/2020, 131-148.
28. Van der Sloot, B., *Regulating the Synthetic Society*, Hart Publishing, Oxford 2024
29. Van der Sloot, B.; Wagenveld, Y., *Deepfakes: regulatory challenges for the synthetic society*, Computer Law and Security Review, volume 46, 9/2022, 1-15.
30. Von Sikorski, Ch.; Hameleers, M., *Disinformation in the Age of Artificial Intelligence (AI): Implications for Journalism and Mass Communication*, Journalism & Mass Communication Quarterly, volume 102, 11/2025, 941–957,
31. Weikmann, T.; Egelhofer, J.; Lecheler, S., *Beyond Credibility: The Effects of Different Forms of Visual Disinformation*, Journalism & Mass Communication Quarterly, volume 102, 12/2025, 1020-1043.
32. Züger, T.; Asghari, H., *AI for the public. How public interest theory shifts the discourse on AI*, AI & SOCIETY volume 38, 4/2023, 815-828.

LEGAL RULES

1. Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L 2024/1689.
2. Regulation (EU) 2022/2065 (Digital Services Act), OJ L 277/1.

NETWORK RESOURCES

1. Ašmane, K.L; McNamee, J., Malicious semi-compliance as the platform approach to EU regulation, EU DisinfoLab, 25 November, 2025, <https://www.disinfo.eu/malicious-semi-compliance-as-platform-approach-to-eu-regulation/>, 28 February, 2026
2. Berger, E., 'They feel true': political deepfakes are growing in influence – even if people know they aren't real, The Guardian, 28 March, 2026, <https://www.theguardian.com/technology/2026/mar/28/military-deepfakes-ai-propaganda-money>, 1 April 2026.
3. Bertelsmann Stiftung, Decentralized Social Media Platforms as a Path to a More Resilient Information Ecosystem, January 2026 <https://www.bertelsmann-stiftung.de>, 28 February 2026
4. Bleyer-Simon, K.; Reviglio, U., Defining Disinformation across EU and VLOP Policies, European Digital Media Observatory, October 2024, p.11, <https://edmo.eu/wp-content/uploads/2024/10/EDMO-Report-%E2%80%93-Defining-Disinformation-across-EU-and-VLOP-Policies.pdf>, 1 April, 2026.
5. Chesney, R.; Danielle, C., *Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?* Lawfare, February 2018, <https://www.lawfaremedia.org/article/deepfakes-looming-crisis-national-security-democracy-and-privacy>, accessed 26 February, 2026.
6. DeepFaceLab, How DeepFaceLab Works, <https://deepfacelab.org/#choose>, 31 March 2026.
7. European Commission, Commission fines X €120 million under the Digital Services Act, European Commission Press Corner, 5 December 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934, 1 April, 2026.
8. European Commission, The Code of Conduct on Disinformation, February 2026, p. 1, 2025 <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation>, 26 February, 2026.
9. European Commission, First Draft Code of Practice on Transparency of AI-Generated Content, February 2026, p. 2, <https://digital-strategy.ec.europa.eu/en/library/first-draft-code-practice-transparency-ai-generated-content> 1 March, 2026.

10. European Digital Rights (EDRi), Press Release: EU stands up to Big Tech with €120 million fine to X, 8 December 2025, EDRi Resources, <https://edri.org/our-work/eu-stands-up-to-big-tech-with-e120-million-fine-to-x/>, 1 April 2026.
11. EU Disinfo Lab, About, <https://www.disinfo.eu/about-us/problem/>, 28 February, 2026
12. European Parliament, Tackling AI deepfakes and sexual exploitation on social media (EP) Briefing, European Parliament, 15 January, 2026, <https://www.europarl.europa.eu/news/en/agenda/plenary-news/2026-01-19/8/tackling-ai-deepfakes-and-sexual-exploitation-on-social-media>, 15 February, 2026.
13. Gombar, M.; M. Boban, Research on the Impact of Algorithmic Echo Chambers on Perceptions and Attitudes of Social Network Users in a Digital Society, *MIPRO 48th ICT and Electronics Convention*, Opatija, Croatia, June 2025, <https://ieeexplore.ieee.org/document/11131918>, 1 April, 2026.
14. Kira, B., Deepfakes, The Weaponisation of AI Against Women and Possible Solutions, Verfassungsblog, June 2024, <https://verfassungsblog.de/deepfakes-ncid-ai-regulation/>, 12 February, 2026.
15. Körömi, C.; Haec, P; Cheslow, D, Zuck goes full Musk, dumps Facebook fact-checking program 7 January 2025, POLITICO, <https://www.politico.eu/article/mark-zuckerberg-full-elon-musk-dump-facebook-fact-checker/>, 20 February 2026.
16. Marco Silva, Flood of AI soldiers push pro-Iran messages during war, BBC News, 12 March 2026, <https://www.bbc.com/news/videos/cy9gw900dp9o>, 1 April, 2026.
17. Parker, J.; Völk, K., How deepfake porn scandal surrounding TV star rocked Germany, BBC News, 29 March, 2026, <https://www.bbc.com/news/articles/c9vlm4j47e2o>, 31 March, 2026.
18. Polona, C., Fact-checking and content moderation, European Parliamentary Research Service, February 2025, p. 2, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769493/EPRS_ATAG\(2025\)](https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769493/EPRS_ATAG(2025)), 12 February, 2026.
19. Powers, C., Zuckerberg calls on US to defend tech companies against European 'censorship', Euroactiv, 12 January, 2025, <https://www.euractiv.com/news/zuckerberg-calls-on-us-to-defend-tech-companies-against-european-censorship/>, 26 February, 2026.
20. Shukla, V., Deepfakes and Elections: The Risk to Women's Political Participation, TechPolicy Press, February 2024, <https://www.techpolicy.press/deepfakes-and-elections-the-risk-to-womens-political-participation/>, 20 February, 2026.

21. Twomey, J. J.; Linehan, C.; Murphy, G., Deepfakes in warfare: new concerns emerge from their use around the Russian invasion of Ukraine, The Conversation, October 2023, 2023, <https://theconversation.com/deepfakes-in-warfare-new-concerns-emerge-from-their-use-around-the-russian-invasion-of-ukraine-216393>, 31 March, 2026.

UDK: 004.8 : 347.78 (489 + 735)
34 : 007 (4-67 EU)
Review paper

Alexandra Salnikow, PhD student
Faculty of Law, University of Vienna, Austria
E-mail: alexandra.salnikow@univie.ac.at
ORCID-ID: 0009-0004-7290-249X

DEEPFAKES ACROSS JURISDICTIONS: REGULATORY APPROACHES IN TENNESSEE AND DENMARK TO THE PROTECTION OF PERSONAL CHARACTERISTICS

ABSTRACT

Responding to calls from artists' organisations (e.g., the US Screen Actors Guild and Germany's Voice Actors Association), regulators have begun to act, notably with Tennessee's ELVIS Act and Denmark's proposal to amend its Copyright Act to curb the sharing of realistic, digitally generated imitations of personal characteristics and performances. This paper analyses these regulatory responses with a targeted focus on the protection of personal characteristics (image and voice) and measures designed to mitigate risks for artists and performers. It contrasts Tennessee's explicit consent-based protection (including voice) with Denmark's copyright-anchored draft that effectively codifies personality-control norms while raising questions of fit, effectiveness against fully synthetic deepfakes, and compliance with EU copyright harmonisation. The paper argues that coherent safeguards for artists require clear consent defaults for image and voice and careful alignment with EU law – offering lessons for Member States and, ultimately, for a more coordinated EU and global approach to governing deepfakes ethically and responsibly.

Keywords: *deepfakes, image and voice protection, EU law, regulatory responses, artificial intelligence*

1. INTRODUCTION

Deepfakes are AI-generated synthetic media that can convincingly imitate individuals. This technology has sparked a worldwide discussion on how to address its risks. It gained prominence in 2017 with a Reddit user (username 'deepfakes') who edited the faces of famous actresses and singers into

pornographic videos and uploaded them to the platform.¹ The term² is likely a hybrid of 'deep learning', referring to the fact that deepfakes are usually created with deep learning technology which is a form of artificial intelligence, and 'fake', reflecting the deceptive deceitful nature of deepfakes, which may appear to be authentic, while being completely synthetic.

This negative connotation of the term also reflects the dangers deepfake technology poses. Although the technology as such may not be inherently harmful, it lends itself to many harmful uses³, as illustrated by cases of deepfake-based disinformation and the rise of deepfake pornography. As early as 2019, over 90% of deepfake videos online contained pornographic content.⁴ This trend has remained unchanged, as evidenced by incidents with the AI tool Grok. Of the millions of images generated over nine days, at least 41% were sexualised images of women.⁵ Many legislative responses, therefore, target this ongoing problem of non-consensual sexual synthetic imagery, and in light of the incidents with Grok, the EU Parliament included recommendations⁶ to include provisions on the protection against deepfake pornography in the Digital Omnibus.

¹ The original website on Reddit can still be seen on the waybackmachine, even if the videos have been deleted in the meantime. Waybackmachine, Webpage of the Reddit user 'deepfakes' on 17 December 2017, <https://web.archive.org/web/20171212214356/https://www.reddit.com/user/deepfakes/submitted/>, 26 March 2026.

² It is quite interesting that not every language chooses to incorporate the English neologism in their language, some languages create their own. This best can be observed when looking at Art 3 No. 60 of the AI Act in the different languages. For example, Greek, Spanish or French have created their own neologism to describe AI-generated synthetic media. A table with a comparison of the term provided by the author of this paper, can be found here: Salnikow, A., Term deepfakes in Art. 3 No. 3 of the AI Act in different languages - overview, <https://lush-antelope-62c.notion.site/Term-deepfakes-in-Art-3-No-3-of-the-AI-Act-in-different-languages-overview-315909c4539280199771d169c2f7368c>, 26 March 2026.

³ For an overview of potential misuse of deepfakes see EPRS, *Tackling deepfakes in EU policy*, 4.

⁴ Deeprace, The state of deepfakes: Landscape, threats, and impact, 2019, p. 1, https://regmedia.co.uk/2019/10/08/deepfake_report.pdf, 26 March 2026.

⁵ Conger, K.; Stuart, A., *Elon Musk's Grok A.I. Chatbot Made Millions of Sexualized Images, New Estimates Show*, The New York Times, 22 January 2026, <https://www.nytimes.com/2026/01/22/technology/grok-x-ai-elon-musk-deepfakes.html>, 26 March 2026.

⁶ See Amendments 171 to 176 which suggest including sexual AI imagery as a forbidden practice in Art 5 AI Act and Amendments 253 to 254 which suggest obliging the providers of AI systems in Art 50 AI Act to include measures to prevent the generation of deepfakes depicting non-consensual nudity or sexually explicit conduct. Kokalari A. and McNamara, Amendments 171-317: Draft Report on the Proposal for a Regulation of the EU Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence

At the same time, deepfake technology offers significant positive applications, for example, in political and social satire, marketing, research, and psychological care.⁷ In the entertainment and music industry, deepfake technology may enable artists to license their face or voice in new ways. Some well-known celebrities already offer their voices on voice-generation websites for public use.⁸ With the current technology, it is easy to realistically replicate the voice or appearance of a person with minimal source material. Currently, as little as a three-second audio sample is sufficient to generate a realistic audio imitation (deepfake) of a person's voice.⁹ This poses a threat to a person's autonomy over their personal characteristics. This concern over autonomy poses a challenge for the creative sector, as artists — such as actors, singers, and musicians—fear their work will be used without their consent or compensation. The Writers Guild of America and SAG-AFTRA early drew attention to the potential harm of AI – including deepfakes – for the creative sector.¹⁰ This raised awareness in artists' associations all over the world. For example, the German Voice Actor Association¹¹ opened discussions on the right to one's own voice with the streaming platform Netflix, temporarily refusing further collaboration. The starting point was a new contract provided by Netflix that would have included an 'AI clause'. This clause would have allowed Netflix to use all audio recordings for AI training. The German Voice Actors Association criticised the lack of choice, as Netflix refused further voice actor employment without signing the AI clause. Furthermore, no additional remuneration was offered.¹²

(Digital Omnibus on AI), (COM(2025)0836 – C10-0304/2025 – 2025/0359(COD)), 14 February 2026 2025/0359(COD).

⁷ For an overview of potential positive uses of deepfakes see Westerlund, M., *The Emergence of Deepfake Technology: A Review*, TIm Review, 11/ 2019 9, 41.

⁸ For example, the voices of Snoop Dogg, Mr. Beast and Gwyneth Paltrow are available on 'Speechify' with these celebrities' permission. Weitzman, C., Voicify AI: Revolutionize Your Voice Content Creation, Speechify, 2025, https://speechify.com/blog/voicify-ai/?srsltid=AfmBOOpNiUWFuwKT48azT29mK0DEuXIkmt7GY-JEIV4EJqFgiphr_k_, 26 March 2026.

⁹ See Microsoft Research, VALL-E, 09 May 2025, <https://www.microsoft.com/en-us/research/project/vall-e-x/>, 26 March 2026.

¹⁰ Barnes, B. *et al.*, *Hollywood Actors Join Writers on Strike, Bringing Industry to a Standstill*, The New York Times, 13 July 2023, <https://www.nytimes.com/2023/07/13/business/media/sag-aftra-writers-strike.html>, 26 March 2026.

¹¹ VDS – Berufsverband für professionelle Sprecher:innen, <https://www.sprecherverband.de/>, 26 March 2026.

¹² Rbb, J.S., Streit mit Netflix: Synchronsprecher protestieren gegen KI-Klausel, tagesschau.de, 8 February 2026, <https://www.tagesschau.de/wirtschaft/synchronsprecher-netflix-ki-100.html>, 26 March 2026.

In an interview, Patrick Winczewski – the voice actor for Hugh Grant and Tom Cruise – emphasised that the technology is already part of society and in use.¹³ To name a few examples, the use of AI technology to recreate the voice of deceased voice actor Hans Joachim Clarin in a new iteration of the series 'Neue Geschichten vom Pumuckl' can be mentioned.¹⁴ Winczewski, however, stressed that choice and autonomy are vital for the future of the voice actor as well as the whole creative industry. The German Voice Actor Association, therefore, calls for a right to choose freely whether to use AI, including the right to refuse, and for an open discussion of new forms of remuneration in the age of AI. The association has commissioned a legal opinion ('Rechtsgutachten') which concludes that the forced approach adopted by Netflix is unlawful.¹⁵ However, as the feeling of legal uncertainty regarding the topic of deepfakes remains, there is a call for regulation of the phenomenon.

There are two notable legislative responses to these concerns of artists. The most prominent legislation in this regard is the so-called ELVIS Act of the US state of Tennessee, as it can be considered the first law to target deepfakes by broadening the protection of the right to publicity. In Europe, Denmark has taken another approach, by planning to introduce protection against realistic digital imitation into its Copyright Act. The legislative proposal of Denmark is still pending at the time of writing but offers an interesting approach regarding deepfakes.

2. METHODS OF THE PAPER

This paper examines the Tennessean and Danish legal approaches to protecting artists and performers from deepfake imitations of personal characteristics, using a comparative doctrinal case-study approach. The focus is on protection against deepfake imitation—synthetic media that imitate a specific person.¹⁶

After a brief introduction to the technology, the paper discusses first the Tennessean and then the Danish legislative approach. Where appropriate, it makes selective reference to the Austrian (and German) systems of personality rights and

¹³ *Loc. cit.*

¹⁴ Bekommt der Pumuckl wieder die Hans-Clarin-Stimme?, OVB Heimatzeitungen. 31 May 2022, <https://www.ovb-heimatzeitungen.de/rosenheim-region/2022/03/30/bekommt-der-pumuckl-wieder-die-hans-clarin-stimme.ovb?shorten>, 26 March 2026.

¹⁵ Hense, P.; Kahl, J.; Manthey, G.; Wagner, D., *Rechtsgutachten Netflix AI Training: im Auftrag von Verband Deutscher Sprecher:innen e.V.* 2026.

¹⁶ In contrast, the technology of deepfakes can also be used to generate random person who do not resemble a specific person. See for example This Person Does Not Exist - Random Face Generator. 2021-2023, <https://this-person-does-not-exist.com/en>, 26 March 2026.

copyright, whose continental personality-rights structure and copyright regimes comparable to Denmark offer useful comparative insights. Finally, the paper assesses whether the two case studies provide guidance for legislative action to safeguard autonomy over personal characteristics against deepfakes for performers in the EU.

3. DEEPFAKE TECHNOLOGY

Deepfakes constitute a sub-category of AI-generated media.¹⁷ However, the term is not uniformly defined and, therefore, takes on different meanings depending on the context. There are different types of deepfakes. When discussing deepfakes, content is usually meant that was created based on deep neural networks, i.e., artificial intelligence.¹⁸ This AI-based technology makes highly realistic content possible.¹⁹ In contrast, the term 'cheap fakes' can be used to refer to content of inferior quality that may stand up to initial scrutiny but not to closer examination.²⁰

It is even possible to use deep learning technology in isolated (partly synthetic deepfakes). An example is the technique of face replacement (face-swap) that aims to swap the face of a target person to replace the face in a source image or video.²¹ In contrast, completely synthetic deepfakes include no parts of other material, but are created entirely from scratch by AI technology. The possibilities of imitation with deepfake technology are improving, allowing the creation of realistic imitations with just a few clicks.²² In this regard, synthetic deepfake imitation differs significantly from traditional mimicry and copyright reproduction. Traditional voice mimicry is less disruptive than deepfakes, as, for example, a voice impersonator requires a certain level of skill to be a true copy and is physically limited in their use of another person's voice. In contrast, deepfake technology allows for a practically unlimited and highly realistic reproduction of a person's likeness and voice and, therefore, is more harmful.²³ Moreover, deepfakes differ from traditional reproductions of works, which are governed by copyright, as the AI-based technology enables the creation of content that is

¹⁷ EPRS, *Tackling deepfakes in EU policy: Study*, 2021, p. 1.

¹⁸ *Loc. cit.*

¹⁹ For more on the technology behind deepfakes see van der Sloot B. *Regulating the synthetic society: Generative AI, Legal Questions and Societal Challenges*, Bloomsbury Publishing 2024, p. 44ff.

²⁰ *Ibid.*, p. 46.

²¹ *Ibid.*, p. 9.

²² For details see p. 3.

²³ Moos, K., *My Body, My Voice: Defining Vocal Identity Rights to combat AI-Generated Deception*, Mar Intell Prop Innovation L REv. 29(2) 2025, 358.

entirely novel and does not incorporate any copyright-protected aspects in the output (the deepfake).²⁴ Against this technical background, legislators in Tennessee and Denmark have introduced or have sought to introduce protections against this technology.

4. TENNESSEE: ELVIS ACT

A prominent example of strengthening the protection of personal characteristics against deepfakes can be found in the US state of Tennessee. The Ensuring Likeness Voice and Image Security Act²⁵—ELVIS Act for short—was the first US legislation to specifically protect artists and musicians from the unauthorised use of their likeness and voices through AI technologies and against deepfakes. It aims to achieve this by broadening the statutory right to publicity.

4.1. History of the ELVIS Act

The ELVIS Act was passed on 21 March 2024 and went into effect on 1 July 2024.²⁶ It is not a novel law, but an amendment to the 'Personal Rights Protection Act of 1984'. The acronym of the Act referring to the well-known musician is no coincidence but goes back to the background of the amended law. It is sometimes stated that '*Tennessee's right of publicity was not just developed because of Elvis, it was developed for Elvis*'²⁷. This is not entirely accurate, as the doctrinal evolution of the right of publicity itself cannot be traced back to the well-known artist.²⁸ The name of the Act of 2024 is probably inspired by the history behind the preceding Personal Rights Protection Act of 1984, which was enacted in response to a court decision regarding Elvis Presley's heirs—the Elvis Presley Estate which inherited Elvis' independent right to publicity after his death. Legal Cases in the 1980s following Elvis Presley's death shaped the right of publicity in Tennessee. In a court case²⁹ involving the Elvis Presley Estate, it

²⁴ van der Sloot, *op. cit.* note 22, p. 47.

²⁵ Ensuring Likeness Voice and Image Security Act - Tennessee Senate Bill 2096 (112th General Assembly), 07 March 2024.

²⁶ ELVIS Act, Section 12, 13.

²⁷ Christoff, A.T., *Long Live the King: The Influence of Elvis Presley on the Right of Publicity in Tennessee*, U. Mem. L. Rev., 41/2011, p. 667.

²⁸ Moldawer, M., *ELVIS Act: From Authorship to Ownership in Intellectual Property Law*, Texas Intellectual Property Law Journal 2024, p. 21.

²⁹ State ex rel. Elvis Presley Int'l Mem. Found. v. Crowell 733 S.W.2d 89, 95 (Tenn. Ct. App. 1987), discussing Memphis Dev. Found. v. Factors, Etc. Inc. 441 F. Supp. 1323, 1330 (W.D. Tenn. 1977).

was held that the law did not provide for a right to publicity that survived a celebrity's death. Therefore, protection for the Elvis Presley Estate was denied. The Tennessee General Assembly aimed to correct this outcome, recognising the need for a post-mortem right to publicity. Consequently, the Personal Rights Protection Act of 1984 was enacted, providing protection for a person's name, photograph, or likeness that continued after the individual's death and that also can be passed on to their family or heirs.³⁰

4.2. Deepfakes and the right to publicity

The doctrinal evolution of the right of publicity started with the privacy-based 'right to be left alone' that subsequently developed into a transferable property right of celebrities to their personal features.³¹ The right of publicity is often defined as 'the right to stop others from using [one's] identities, particularly [one's] names and likenesses, without permission'.³² In the US, there is no federal or constitutional right to publicity, but it is created at state level in common and/or statutory law, resulting in a fragmented legal landscape.³³ However, protection against the commercial appropriation of an individual's name or likeness can be identified as a common ground.³⁴ In Tennessee, even prior to the ELVIS Act, the 'Personal Rights Protection Act of 1984' offered a statutory right of publicity.³⁵ This framework was, however, deemed ineffective against AI-generated imitations. One aspect was the lack of protection of the voice. Tennessee law – like many US states – only offered individuals a property right in the use of that person's name, photograph, or likeness.³⁶ The lack of protection of the voice in current US personality rights was a major point of concern, as deepfake technology has made highly realistic voice cloning possible.³⁷ The ELVIS Act addressed this problem by being one of the first US states to introduce an explicit protection of the voice. Another point of concern was the synthetic nature of

³⁰ Christoff, *op. cit.* note 31, p. 691f. The descendibility of the right to publicity was also recognized under common law by the Tennessee Court of Appeal three years after the enactment of the Personal Rights Act of 1984. See *Ibid.*, p. 693, citing *Elvis Presley v. Crowell*, *op. cit.* note 33.

³¹ For details on this evolution see Moldawer, *op. cit.* note 32, p. 21ff.

³² Rothman, J., *The Right of Publicity: Privacy Reimagined for a Public World*, Harvard University Press 2018, p. 2.

³³ *Ibid.*, p. 3f.

³⁴ Preminger, A.; Kugler, M., *The Right of Publicity Can Save Actors From Deepfake Armageddon*, BTLJ, 39/ 2023, p. 794.

³⁵ Christoff, *op. cit.* note 31, p. 691f.

³⁶ Fowler, S.L.; Fowler, J.D., *Why Tennessee's ELVIS Act Is the King of Artificial Intelligence Protections*, *Vand. J. Ent. & Tech. L.*, 27(2)/2025, p. 263.

³⁷ Moos, *op. cit.* note 26, p. 355.

AI-generated content. Case law suggested that the right of publicity may not apply if the imitation of a person's likeness or voice cannot be attributed to a specific individual. In the case of *Midler v. Ford Motor Co.*, the singer Midler claimed to be imitated by a similar-sounding vocalist after Midler had been denied a contract with Ford to create the said commercial jingle. The court held that the statutory right of publicity did not apply because Midler's voice was not 'used' but merely imitated.³⁸ Some authors, therefore, doubted the applicability of the right of publicity to AI-generated images and recordings, arguing that they similarly may not constitute a use of a person's personal characteristics but only imitations of an individual.³⁹ Others argue that AI-generated imitations constitute an appropriation of likeness and voice covered by the right of publicity, pointing to the case of traditional CGI.⁴⁰ In *Hart v. Electronic Arts*, the court determined CGI depictions in video games to be a use of likeness when digital avatars mirror real individuals.⁴¹ This legal uncertainty—whether AI-generated imitation will be covered by the statutory right of publicity—was the motivation for the adoption of the ELVIS Act.⁴²

The Act now imposes liability where, without the individual's prior consent, a person publishes, performs, distributes, transmits, or otherwise makes available to the public an individual's voice or likeness, without the required consent.⁴³ Moreover, a person is also liable for the distribution, transmission, or making available of an 'algorithm, software, tool, or other technology, service, or device, the primary purpose or function' of which is 'the production of a particular, identifiable individual's photograph, voice, or likeness'⁴⁴ without consent.

4.3. Critique

On the one hand, blind spots in the right of publicity have been brought to attention. Despite the ELVIS Act providing broad protection for personal characteristics, only certain uses are prohibited ('purposes of advertising products, merchandise, goods, or services, or for purposes of fundraising, solicitation of donations, purchases of products, merchandise, goods, or services'⁴⁵). The

³⁸ The court, however, still found the defendant liable for common law misappropriation claim. See *Midler v. Ford Motor Co.* 849 F.2d 460 (9th Cir. 1988) at 463.

³⁹ See Moos, *op. cit.* note 26, p. 355.

⁴⁰ Preminger *et al.*, *op. cit.* note 38, p. 799f.

⁴¹ *Hart v. Elec.Arts, Inc.* 717 F.3d 141, 147 (3rd Cir. 2013).

⁴² Moos, *op. cit.* note 26, p. 357f.

⁴³ ELVIS Act Section 6(a)(2).

⁴⁴ *Ibid.*, Section 6(a)(3).

⁴⁵ *Ibid.*, Section 6(a)(1).

limitation to commercial uses creates uncertainty regarding deepfakes distributed on the internet. For example, the commercial aspect of the use of social media may be less clear than a film studio using an actor's face for a deepfake replica without their consent.⁴⁶ Non-commercial deepfakes fall outside the scope of the ELVIS Act and most other statutory publicity rights.⁴⁷

On the other hand, the scope of protection was also deemed too broad. For example, voice as a medium is protected if it is 'readily identifiable and attributable to a particular individual, regardless of whether the sound contains the actual voice or a simulation of the voice of the individual'⁴⁸. This would, therefore, not only include AI-generated imitations, but also traditional voice mimicry, as seen in *Midler v. Ford*. As AI generation is not comparable to traditional mimicry, the scope of protection should be calibrated, introducing a tiered level of protection that is justified by the specific risk to the imitation of personal characteristics.⁴⁹

4.4. Ownership of personal characteristics?

Due to its strong protection, the right of publicity under the ELVIS Act is classified as a property-based, IP-like⁵⁰ right to one's name, voice, and likeness. This is strongly supported by the legal text which states that '[e]very individual has a property right in the use of that individual's name, photograph, voice, or likeness in any medium in any manner.'⁵¹ The right of publicity in general is widely recognised as a form of intellectual property.⁵² Occasionally, it is described as a 'legal hybrid, zigzagging between privacy, property rights, trademark law, and copyright law'⁵³. A major point of critique is that the ELVIS Act's right of publicity awards ownership to personal characteristics similarly to copyright, without inciting a similar discussion on the struggle to balance authorship rights and the freedoms of the public domain.⁵⁴

⁴⁶ For a deeper discussion see Preminger *et al.*, *op. cit.* note 38, p. 805ff.

⁴⁷ See for example the California Civil Code. Section 3344 and New York Laws Civil Rights. L (Consol. 20239). Section 50. In this regard, California's common law is an exemption as it extends the scope to noncommercial uses as well (See *White v. Samsung Electronics America Inc.* 971 F.2d 1395, 1401 (9th Cir. 1992) at 1397).

⁴⁸ Tennessee Code Annotated Section 47-25-1102.

⁴⁹ See Moos, *op. cit.* note 26, p. 358.

⁵⁰ Moldawer, *op. cit.* note 32, p. 65f.

⁵¹ Tennessee Code Section 47-25-1103(a).

⁵² See e.g. *Zacchini v. Scripps-Howard Broad. Co.* 433 U.S. 562, 573 (1977). For more details see Fowler *et al.*, *op. cit.* note 40, p. 277; Moldawer, *op. cit.* note 32, p. 21ff; Preminger *et al.*, *op. cit.* note 38, p. 793f; Rothman, *op. cit.* note 36, p. 75ff.

⁵³ Moldawer, *op. cit.* note 32, p. 35.

⁵⁴ *Ibid.*, p. 23.

The ELVIS Act does not prohibit every use of personal characteristics but provides a fair-use exception that applies to uses of name, photograph, voice, or likeness (1) in news, public affairs, or sports broadcasts; (2) for comment, criticism, scholarship, satire, or parody; or (3) for the 'representation of the individual as the individual's self in an audiovisual work, [...] unless the audiovisual work containing the use is intended to create, and does create, the false impression that the work is an authentic recording in which the individual participated'; (4) for fleeting or incidental uses; and (5) for an advertisement or commercial announcement for any of the above.⁵⁵ These exceptions reflect the need to balance protection against deepfakes with fundamental rights such as the right to freedom of expression.⁵⁶ However, the narrow wording of the exception raises concerns that while the ownership over personal characteristics is strengthened, the freedom of the public is restricted. This creates the curious paradox that the attempt to strengthen the protection in reaction to a new technology may create the very framework that encourages further exploitation.⁵⁷ This conflict between wanting to protect personal characteristics against deepfakes and needing to balance this protection with the freedom of others lies at the core of the problem of regulating new technologies.

4.5. Inspiration for Europe?

The ELVIS Act could serve as a source of inspiration for future legislation, as it aims to strengthen legal protection against deepfakes. The lack of protection of personal characteristics – especially the voice – is also a problem in Europe. However, the critique of the Tennessean law also demonstrates the risk of simply establishing ownership over personal characteristics without establishing a balance with the rights of the public, such as the freedom of expression or art. The scope of legislation targeted at AI-generated media also must be considered, as it may accidentally cover cases such as traditional mimicry, which do not pose the same harm as deepfakes. Moreover, for transposing such protection into Member States' national or even EU law, the features of the legal systems have to be considered. Tennessee, having a different legal framework, especially regarding the doctrinal structure of the right of publicity, may not fit (all) European countries. In this regard, further research will be needed before crafting a draft for the protection of personality rights for the EU and/or Member States. For example, the GDPR plays an important role in EU countries. Since the personal

⁵⁵ Tennessean Code Section 47-25-1107(a).

⁵⁶ See Moos, *op. cit.* note 26, p. 361.

⁵⁷ Moldawer, *op. cit.* note 32.

characteristics of deepfakes can constitute personal data, the relationship between the GDPR and EU legislation must be considered. There are also regulatory proposals that address data protection directly. Notably, the '*right not to be cloned*'⁵⁸ in the draft of C. Wendehorst is worth mentioning here.

The need for legislation was also not left unanswered in Europe. In October 2025, Denmark released a legislative draft to strengthen protection against deepfakes, not as an amendment to data protection regulation, but to its Copyright Act.⁵⁹

5. DENMARK: AMENDMENT OF THE COPYRIGHT ACT

The Danish Government released a legislative proposal to amend the Danish Copyright Act, intending to create a safeguard against digitally generated imitations (hereinafter, the 'Danish Draft')⁶⁰.

5.1. History

The legislative proposal reflects a political agreement of 26 June 2025 between the Danish Government and a broad spectrum of parties in the Danish Parliament.⁶¹ On 7 October 2025, the Danish Government submitted a written

⁵⁸ Art. 12 (2) (b) (ii) of the Tentative Academic Discussion Draft (version 1.1.) for a Regulation on the protection of personal data in the context of artificial intelligence and the data economy and amending Regulation (EU) 2024/1689 ('AI Data Protection Regulation'). Wendehorst, C., *Datenschutz im Zeitalter von KI: Wissenschaftlicher Diskussionsentwurf für eine neue „KI-Datenschutz-VO“ (Teil 2)*, KIR 2025. The draft is also included in the response of the ELI on the Digital Package which is available here: ELI, *Simpler, Fairer, More Effective – Towards a Targeted Revision of EU Data Protection law*, https://www.EUlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_-_Simpler_fairer_more_effective.pdf, 26 March 2026.

⁵⁹ Kulturministeriet, Deepfakes, produktionsrabat og mindre bureaukrati er på årets lovprogram, 07 October 2025, <https://kum.dk/aktuelt/nyheder/deepfakes-produktionsrabat-og-mindre-bureaukrati-er-paa-aarets-lovprogram>, 26 March 2026.

⁶⁰ The text of the legislative proposal including explanatory notes of the Danish Government (in Danish and English) are provided in the TRIS notification of Denmark to the Commission and can be accessed here: <https://technical-regulation-information-system.ec.europa.eu/en/notification/27420>, 26 March 2026.

⁶¹ The political agreement included the government consisting of the Social Democrats, Liberal Party and Moderates. Of the parties in parliament, the Denmark Democrats, Socialist People's Party, Conservative People's Party, Red-Green Alliance, Danish Social Liberal Party and the Alternative joined. Kulturministeriet, Bred aftale om deepfakes giver alle ret til egen krop og egen stemme, 06 June 2025, <https://kum.dk/aktuelt/nyheder/bred-aftale-om-deepfakes-giver-alle-ret-til-egen-krop-og-egen-stemme>, 06 June 2025.

draft to the Danish Parliament for review that corresponded with the political agreement.⁶² At the time of writing, the bill is still under review.

The Danish Government also notified the EU Commission of the planned legislation in accordance with the notification procedure under Directive (EU) 2015/1535 (TRIS – Technical Regulation Information System).⁶³ The notification procedure obliges Member States to notify the Commission of any draft technical regulation prior to its adoption. The notification triggers a three-month standstill period during which the notifying Member State cannot adopt the technical regulation in question. This enables the Commission and the other Member States to examine the notified text and to respond appropriately.⁶⁴ In this instance, the Commission reacted to the Danish Draft with comments only.⁶⁵ The draft can, therefore, be adopted after the expiration of the three-months-standstill-period if Denmark incorporates the Commission's comments accordingly. As will be seen in the analysis of the draft (chapter 5.3), Denmark will have to adapt the draft, as the Commission drew attention to incompatibilities with EU directives.

5.2. Content of the Draft

The Danish Government provided the draft of the amendment to the Danish Copyright Act (with English translations) including explanatory notes with their notification in accordance with TRIS.⁶⁶ According to the explanatory notes, the main objective of the Danish legislative proposal is to provide protection against the abuse of personal characteristics and to ensure that technological developments like AI that enable the creation of realistic representations of individuals, their

aftale-om-deepfakes-giver-alle-ret-til-egen-krop-og-egen-stemme, 26 March 2026. Details on the political proposal can be found here: Kulturministeriet, Værn mod deling af digitale efterligninger af personlige kendetegn, 26 June 2025, [https://kum.dk/fileadmin/kum/1_Nyheder_og_presse/2025/Vaern_mod_deling_af_digita le_efterligninger.pdf](https://kum.dk/fileadmin/kum/1_Nyheder_og_presse/2025/Vaern_mod_deling_af_digita_le_efterligninger.pdf), 26 March 2026.

⁶² Kulturministeriet, *op. cit.* note 65.

⁶³ EU Commission, Act amending the Copyright Act (Introduction of performance protection and protection against digitally generated imitations, etc.): Notification Detail, 31 October 2025, <https://technical-regulation-information-system.ec.europa.eu/en/notification/27420>, 26 March 2026.

⁶⁴ Directive (EU) 2015/1535 of the EU Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification).

⁶⁵ EU Commission, *op. cit.* note 69.

⁶⁶ The text of the Danish Draft (with explanatory notes) can be downloaded here: <https://technical-regulation-information-system.ec.europa.eu/en/notification/27420>, 26 March 2026.

performances, and other characteristics do not come at the '*expense of integrity, credibility, trust, and transparency*'⁶⁷. The draft introduces two additional provisions in the Danish Copyright Act.

§⁶⁸ 65a extends the existing protection of performances for performers under neighbouring rights to the context of deepfakes; the text reads as follows:

Realistic digitally generated imitations of a performer's performance or an artist's artistic presentation may not be made available to the public without the consent of the performer or artist.

(2) The protection provided for in the first paragraph lasts until 50 years have elapsed after the year of death of the performer or artist.

(3) The provisions of [§] 2(3) and (4), [§§] 3, 11, 13, 13a, 16a, 16c-16f and 17-17b, [§] 17c(2), (3) and (4), [§§] 17d-17e, [§] 18(1) and (2), [§] 19(1) and (2) and [§§] 21-23, 24b, 25, 25a, 27, 28, 30a, 33, 34, 35, [§] 47(1) and (2), [§§] 49, 50-57, 58a, 61 and 62 apply mutatis mutandis to realistic digital imitations of performers' performances or of artists' artistic presentations.'⁶⁹

As this provision will introduce the terms '*artist*' and '*presentation*' in addition to the existing ones '*performer*' and '*performance*', the draft stipulates that this new term is to be added to other provisions of the Danish Copyright Act.⁷⁰

§ 73a, in contrast, takes a more innovative approach, introducing protection against realistic digitally generated imitations of personal characteristics for the general public into a Copyright Act; it reads as follows:

Realistic digitally generated imitations of a physical person's personal physical characteristics may not be made available to the general public without the consent of the person being imitated.

(2) The first paragraph does not apply to imitations that are mainly expressions of a caricature, satire, parody, pastiche, criticism of power, social criticism, etc. unless the imitation constitutes misinformation that may specifically seriously jeopardise the rights or essential interests of others.

(3) The protection referred to in the first paragraph lasts until 50 years after year [sic!] of death of the person being imitated.

(4) Realistic digitally generated imitations may be made available without consent in accordance with the provisions of [§] 23(2) and [§] 25.⁷¹

Correspondingly, § 86a under the heading '*Special provision on protection against realistic digitally generated imitations of personal characteristics*' specifies that

⁶⁷ Danish Draft, p. 7.

⁶⁸ Where the English translation of the Danish Draft uses 'section', this article retains the section sign (§) of the Danish original.

⁶⁹ Danish Draft § 1 No. 9.

⁷⁰ See *Ibid.*, § 1 No. 2, 5-8.

⁷¹ *Ibid.*, § 1 No. 11.

'[t]he provision in [§] 73a applies to imitations of all natural persons, including foreign nationals.'⁷²

5.3. Critical discussion

The prospect of granting more control over the use of personal characteristics such as voice and image in light of deepfakes seems especially appealing. Therefore, the draft of the Danish Government triggered a discussion whether intellectual property law is an appropriate tool to achieve the intended protection and whether this approach could be a template for the EU.⁷³

This analysis proceeds as follows. First, it examines the choice to place the protection of personal characteristics in the Copyright Act. Second, it considers the balancing of the proposed protection with freedom of expression and related public-interest exceptions. Third, it assesses the effectiveness of the proposed mechanisms. Finally, given partial harmonisation of copyright and neighbouring rights, it considers the draft's compatibility with existing EU law.

5.3.1. Placement within the Copyright Act

A major point of discussion regarding the Danish Draft is the decision to place the protection of personal characteristics in copyright law, even though they do not conceptually fall within the scope of copyright.⁷⁴ This argument mainly concerns § 73a of the Danish Draft, namely the introduction of a general protection against realistic, digitally generated imitations of personal characteristics. § 65a, in principle,⁷⁵ is covered by copyright law, as it broadens the existing protection of

⁷² *Ibid.*, § 1 No. 20.

⁷³ See for example EPRS, The Danish approach to copyright and deepfakes: A model for the EU?, January 2026, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782611/EPRS_ATA\(2026\)782611_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782611/EPRS_ATA(2026)782611_EN.pdf), 26 March 2026.

⁷⁴ Pérez, G.E.M.; Castro, L.H., *Copyright or personality rights? A critical analysis of Denmark's approach to deepfakes*, IDP Revista de Internet, Derecho y Política 2026; EU Commission, *Issue of comments pursuant to Article 5(2) of Directive (EU) 2015/1535 of 9 September 2015 - Notification 2025/0654/DK - Act amending the Copyright Act (Introduction of performance protection and protection against digitally generated imitations, etc.)*, C(2026) 756 final, 2026, p. 7; EPRS, *op. cit.* note 79, p. 2.

⁷⁵ Concerning § 65a Danish Draft, there are however doubts if it is truly just trying to broaden performers protection or if it also in reality also aims at a protection of personal traits. For this discussion see chapter 5.3.4.

performers under neighbouring rights which are partly harmonised by EU copyright directives.⁷⁶

§ 73a explicitly prohibits the imitation of a natural person's personal physical characteristics. Personal characteristics or traits such as a person's image or voice are usually considered intangible aspects of personality – such as ideas or facts, or techniques. These are normally not governed by copyright protection, as they do not constitute a copyright-protected work.⁷⁷

The Danish Government appears to address this aspect in their explanatory notes to the draft. They admit that the right to a person's own image serves a different purpose from protection against imitation under the Copyright Act. However, this statement does not address the distinction between the protection of personal traits and an original copyright-protected work because in the next paragraph a copyright provision on commissioned portraits is cited which provides a limitation to a photographer's rights.⁷⁸ In jurisdictions with continental personality rights, like Germany or Austria, the provision on commissioned portraits is supplemented by the right to one's own image (a personality right).⁷⁹

The legal nature of the protection of personal traits in Denmark is, of course, not necessarily comparable to Germany or Austria. An important aspect to consider in this regard is that Denmark largely relies on unwritten principles governing the use of personal images.⁸⁰ According to the explanatory notes to the Danish Draft, '[i]t follows, firstly, that the commercial use of a person's image may not take place without that person's consent and, secondly, that both publicly known persons and private persons may, depending on the circumstances, are entitled to compensation for non-material damage if the publication of a picture of that person constitutes an unlawful infringement.'⁸¹ The only written provision can be found

⁷⁶ The protection against imitation for performers is partly harmonised by Directive 2001/29/EC (InfoSoc Directive), Directive 2006/115/EC (Rental and Lending Right Directive), Directive 2011/77/EU (Term of Protection Directive), Directive 2014/26/EU (Collective Rights Management Directive) and the Directive (EU) 2019/790 (Copyright in the Digital Single Market Directive).

⁷⁷ Beverley-Smith, H.; Ohly, A.; Lucas-Schloetter, A., *Privacy, Property and Personality*, Cambridge University Press 2009, p. 159; EPRS, *op. cit.* note 20, p. 40.

⁷⁸ Danish Draft p. 9.

⁷⁹ Austria: Ciresa, M., § 75 UrhG in Ciresa, M. (ed), *Österreichisches Urheberrecht*. Wien 2015, Mn. 8. Germany: Loewenheim, U. (ed), *Handbuch des Urheberrechts*, C.H. Beck 2021, Mn. 71ff.

⁸⁰ 'In the current Copyright Act, there are no rules on the protection of personal physical characteristics of natural persons.' Danish Draft p. 44.

⁸¹ *Loc. cit.*

in the Danish Marketing Practices Act, which 'provides protection against the commercial use of personal images without consent'⁸², and in criminal law.⁸³

The Danish Draft even states in the explanatory notes that one of the new provisions cannot be designated as copyright.⁸⁴ This seems to refer to § 65a. They go on to state that the other provision falls 'within the scope of personal rights'⁸⁵. This must refer to § 73a. Another indicator that the Danish Government considers this provision as a personal right and not a matter of copyright is the following statement: 'Personal characteristics are closely linked to a person's personality. For this reason, it is proposed that this area be not covered by an agreement [meaning contractual] licence.'⁸⁶

The objects of protection of § 73a functionally are, therefore, personal characteristics such as voice, movements, and appearance. Such aspects of individual identity do not fall within the scope of the copyright framework, as copyright is designed to protect original expressions of human intellect.⁸⁷ This was also correctly noted by the Commission in its comments.⁸⁸ The copyright framework is unsuitable for the protection of aspects of personal identity for several reasons. Copyright law governs works or performances which are the product of human intellect and require a certain amount of creativity. In contrast, the protection of personal traits constitutes a part of an individual's identity which does not result from creation. Simply extending copyright protection to personal traits without any adjustments to the scope would disrupt the copyright framework, as the temporary monopoly of creators in copyright is balanced with the limitation that protection covers only original intellectual creations.⁸⁹

From a comparative perspective, § 73a of the Danish Draft faces similar criticism to the extension of the right to publicity in the ELVIS Act.⁹⁰ Strengthening the control over personal traits to the same extent as copyright-protected creations disrupts the current framework and unjustifiably limits the freedom of the public. This argument is supported by the rationale of copyright law, which is based on

⁸² *Loc. cit.*

⁸³ *Ibid.*, p. 9ff.

⁸⁴ *Ibid.*, p. 36.

⁸⁵ *Loc. cit.*

⁸⁶ *Ibid.*, p. 19.

⁸⁷ See for example Berne Convention for the Protection of Literary and Artistic Works. September 9 1886, as revised at Paris, July 24 1971, and amended in 1979. Art. 2.

⁸⁸ EU Commission, *op. cit.* note 80, p. 5f.

⁸⁹ Pérez *et al.*, *op. cit.* note 80, p. 4.

⁹⁰ See chapter 4.4.

economic interests.⁹¹ In contrast, the Danish Draft clearly aims for the protection against unauthorised use of personal traits and the prevention of 'a business model based on the commercialisation of images'⁹², explicitly precluding the possibility of licensing⁹³. As observed regarding the ELVIS Act,⁹⁴ using the copyright framework for personal characteristics to protect from unauthorised commercial use may create the paradox that it makes the commercial exploitation of personal traits with deepfakes even more attractive.⁹⁵

With the unsuitability of the copyright framework in mind, the Commission,⁹⁶ as well as literature,⁹⁷ suggested introducing the protection of personal traits against deepfakes within another legal framework. The most prominent candidate in this regard is frameworks for the protection of personality rights.⁹⁸ As mentioned, Danish law relies on unwritten rules for the protection of personal traits; the Danish Draft would function as a codification of those rules.

The placement of such a codification of personality rights in the Copyright Act (provided that it does not rely on a copyright framework) may not seem so unusual from a comparative perspective in Austria. Austrian personality rights are governed by a system of written and unwritten legal principles.⁹⁹ Interestingly, the provision of the right to one's own image, which is considered a personality right, can be found in the Austrian Copyright Act due to historical reasons. When this right was incorporated into legislation, it was considered akin to copyright and therefore included in the Copyright Act.¹⁰⁰ A similar line of argument can be found in the explanatory notes to the Danish Draft by the Danish Government:

'Given that the protection is closely related to protection against realistic digital imitations of performers' performances and artists' artistic

⁹¹ For a detail analysis of the teleological argument against the Danish copyright-based approach see Pérez *et al.*, *op. cit.* note 80, p. 5f.

⁹² *Ibid.*, p. 6 fn. 18.

⁹³ See Danish Draft p. 19.

⁹⁴ See Moldawer, *op. cit.* note 32, p. 25.

⁹⁵ Pérez *et al.*, *op. cit.* note 80, p. 6f.

⁹⁶ EU Commission, *op. cit.* note 80, p. 5f.

⁹⁷ Pérez *et al.*, *op. cit.* note 80, p. 7ff.

⁹⁸ For example, Pérez and Castro suggest the Spanish Organic Act 1/1982, of 5 May, as an inspiration. This Act includes provisions that protects individuals against the use of their name, voice, or image for advertising, commercial or similar purposes. *Ibid.*, p. 9ff.

⁹⁹ Koziol, H.; Warzilek, A., Der Schutz der Persönlichkeitsrechte gegenüber Massenmedien in Österreich in Koziol, H.; Warzilek, A.; Aebi-Müller, R.E. (eds), *Persönlichkeitsschutz gegenüber Massenmedien*, Wien[ua] 2005, Mn. 1ff.

¹⁰⁰ However, this approach of the Austrian legislator has been criticized in literature; for details see Buchner, W., Das Persönlichkeitsrecht des Abgebildeten in Dittrich, R. (ed), *Festschrift 50 Jahre Urheberrechtsgesetz*, Manz 1986, 21f.

performances and presentations, as described in Section 2.2.2 below, and given that the Copyright Act also regulates a large amount of the material on which digital imitations are based – either as work or creations – it is appropriate that this imitation protection be included in the Copyright Act.¹⁰¹

The motivation of the Danish Government to include a non-copyright provision with similarities to copyright in their copyright code is also supported by their intent to change the title of the Danish Copyright Act to 'Copyright etc. Act'¹⁰². The motivation to include a codification of unwritten personality-rights principles within the Copyright Act could also stem from the fact that the Danish legal system possesses no comprehensive civil code which could incorporate such provisions. The other option would be to create a standalone legislative act.

To sum up, the placement of a provision on the protection of personal characteristics (§ 73a) in the Danish Copyright Act can be criticised from a conceptual perspective. The economically motivated copyright framework is not suitable for the protection against deepfakes, with personality-rights frameworks offering a more compatible approach. With a comparative perspective on Austria, the mere placement of such protection in the Copyright Act is less consequential if the structural inconsistencies are dealt with.

5.3.2. Balancing of rights

The Danish Draft – similarly to the ELVIS Act – includes exceptions to the prohibition on the unauthorised imitation of personal characteristics if they constitute 'mainly expressions of a caricature, satire, parody, pastiche, criticism of power, social criticism, etc. unless the imitation constitutes misinformation that may specifically seriously jeopardise the rights or essential interests of others.'¹⁰³ The attempt to balance the protection against deepfakes with the freedom of expression is a welcome addition.

The interpretation of the last part of the sentence in the explanatory notes is, however, noteworthy. The Danish Government seems to suggest that deepfake imitation is excluded from protection if it is disclosed as artificially generated.¹⁰⁴

¹⁰¹ Danish Draft p. 14.

¹⁰² *Ibid.*, p. 36.

¹⁰³ *Ibid.*, § 1 no. 11.

¹⁰⁴ EU Commission, Forwarding of the response of the Member State notifying a draft (Denmark) to request for supplementary information (INFOSUP) of EU Commission

This would mean that labelled deepfake pornography would be outside the scope of the Danish Draft.¹⁰⁵ This contradictory result can be traced back to a misinterpretation of the implications of a transparency label in accordance with the Art. 50(4) of the AI Act.¹⁰⁶ This discussion shows the importance of drafting the public-interest exceptions more carefully.

5.3.3. Copyright protection against deepfakes

Another point of critique is that the Danish Draft cannot provide effective protection against deepfakes, as it wrongly classifies deepfakes as a copyright infringement under the current legal framework. Extending copyright protection and the scope of infringement may prove challenging as well, as the limitations of the applicable EU directives have to be considered (see chapter 5.3.6).

A key problem is that the generated output – in this case, the deepfake – will usually not infringe copyright because it does not reproduce copyright-protected material from its training data. It is essential to distinguish between copyright infringements happening during the training of an AI system and the legality of the output itself.¹⁰⁷ The Danish Draft does not even mention the training phase of deepfake technology and only aims to establish protection against the AI-generated output, the deepfake. If the deepfake does not contain any copyright-protected material, there is no infringement and no grounds for copyright enforcement.¹⁰⁸

The only instance where an area of copyright protection remains is if it is a low-quality 'cheap fake' or a partially synthetic deepfake. However, it must be considered that even in these instances, the depicted person will enjoy no protection under copyright law, as their characteristics are imitated in the synthetic part of the deepfake that is not covered by copyright.¹⁰⁹

(Message number 3402): Notification: 2025/0654/DK, 28 November 2025, p. Answers 10 and 11, <https://technical-regulation-information-system.ec.europa.eu/en/notification/27420>, 26 March 2026.

¹⁰⁵ Pérez *et al.*, *op. cit.* note 80, p. 9.

¹⁰⁶ See EU Commission, *op. cit.* note 80, p. 6f.

¹⁰⁷ Austria: Thurner, A., *Bildmanipulation und Persönlichkeitsschutz in Zeiten von „Deepfakes“*, MR, 4/2019, p. 158f. Germany: Zurth P. *Deepfakes im Kontext des Urheber- und Leistungsschutzrechts*, ZUM 2025, 513.

¹⁰⁸ Zurth, *op. cit.* note 113, p. 513; Mitzscherlich, J., *Das Recht an der eigenen Stimme – Teil 2: Schutz vor ungewollter Kommerzialisierung und KI-Imitation*, AfP 2025, 476f.

¹⁰⁹ Appl, C., *Digitale Identität: Schutz und Verwertung der Persönlichkeit im virtuellen Raum* in Appl, C.; Kreutz, O. (eds), *Daten Information Recht: Festschrift für Andreas Wiebe zum 65. Geburtstag*, Wien 2024. 390.

In light of the rapid technological development, it is a pressing legal problem that there is no protection against highly realistic, completely synthetic deepfakes which contain recognisable personal characteristics of a real person. For this problem, current copyright law offers no solution and may also not be able to do so without challenging the rationale of the current framework. Deepfakes do not infringe a copyright-protected work or an equally protected performance of an artist. Rather, the non-consensual use of the personal characteristics of a person, i.e., appearance or voice, is the point of harm.

5.3.4. Effectiveness of the general protection against deepfakes (§ 73a)

§ 73a of the Danish Draft aims to offer general protection against digitally generated imitation. As discussed, the new rights allocated in the provisions are not strictly copyright, but a personal right to one's own likeness and voice. The placement of the provision in the Copyright Act was already discussed above (see chapter 5.3.1).

Examining effectiveness, a right to control the use of one's personal traits in publicly available digitally generated media can be an effective concept to strengthen autonomy. The Danish approach is very similar to the protection offered by the ELVIS Act in Tennessee, which also intends to establish control (see chapter 0). Similarly to the US state, the lack of written legislation on the protection of all personal characteristics, especially the voice, is a key motivator for legislation.

Some have emphasised that the current legal framework – including the unwritten one – offers sufficient protection.¹¹⁰ This is also a common line of argument, for example, in Austria and Germany where there is a written right to one's own image, but not explicitly the voice.¹¹¹ The protection of voice is commonly accepted in these countries.¹¹² However, legal certainty is a strong argument.

¹¹⁰ EPRS, *op. cit.* note 79, p. 2.

¹¹¹ Austria: Pierer, J., *Künstliche Intelligenz und Persönlichkeitsrecht: Mit Bewährtem gegen Neues*, eclex 2024, 753. Germany: Engel-Bunsas, C., *Das Recht an der eigenen Stimme*, Tectum Verlag 2025; Engel-Bunsas, C.; Lampmann, A., *Recht an der Stimme: ein Normierungsappell aus der Praxis*, GRUR-Prax 2025, p. 109ff.

¹¹² Austria: Dokalik D; Mokrejs-Weinhappel C; Kathrein G. (eds), *Das Große ABGB*, 2025. E 26; Meissel, F.-S., § 16 ABGB in Fenyves, A.; Kerschner, F.; Vonkilch, A. (eds), *Großkommentar zum ABGB - Klang-Kommentar: §§ 1 - 43 ABGB, Methodenlehre und Personenrecht*, Wien[ua] 2014, p. 133. Germany: Frey, D.; Westphal, L., *Rechtlicher Schutz und Verwertung der Stimme als Persönlichkeitsmerkmal: Neue Herausforderungen durch Voice-Cloning-Technologien*, MMR 2025, p. 782; Gomille, C., *Deepfakes und das allgemeine Persönlichkeitsrecht: Der Schutz von Stimme, Bildnis und Selbstdarstellung*,

Given the intent of the Danish Draft, the proposal is undoubtedly a good step in the right direction. The broad wording of the provision and the unsuitable placement within the copyright framework require further discussion of a more balanced approach to the protection against deepfakes.

5.3.5. Effectiveness of protection of performers (§ 65a)

§ 65a of the Danish Draft aims to provide protection for performing artists by extending the existing neighbouring rights to the sharing of realistic, digitally generated imitations of their artistic performances without their consent.¹¹³ The Danish Draft aims to establish more control for performing artists in general (not limited to AI-generated imitations), as the term 'digitally generated' is to be understood broadly, covering not only sophisticated technical means, such as AI, but also less sophisticated technical editing tools.¹¹⁴

Neighbouring rights protect performers, phonogram producers, and broadcasters. The object of protection is performances of works, phonograms, or certain broadcasts. The difference from copyright is the lower threshold of originality of the object of protection. The protected performance still must meet certain criteria for being worthy of protection. They are related to copyright in the sense that they follow the same rationale and have a similar framework. In contrast to the protection of personal characteristics, neighbouring rights still rely on a specific performance, phonogram, or certain broadcast as the object of protection.¹¹⁵

As discussed above, synthetic imitations created by deepfakes usually do not constitute a reproduction of a performance, as they only imitate the personal traits of the person, for example, their voice. In this regard, the Danish Draft remains inconclusive whether the object of protection in § 65a Danish Draft is the (creative) performance of the artist or the personal characteristics of the artist. Only the first falls within the scope of the copyright framework.

The wording of the draft suggests the former, as it regulates 'imitations of a performer's performance or an artist's artistic presentation'¹¹⁶. The explanatory notes of the Danish Government are contradictory. On the one hand, they postulate

ZUM. 2025, p. 506; Wiedemann, M.-J.; Stocks, F., *Der Klang der Zukunft: Die Auswirkungen der KI auf die Musikindustrie*, GRUR 2025, p. 363.

¹¹³ Danish Draft p. 40.

¹¹⁴ *Ibid.*, p. 41.

¹¹⁵ Pérez *et al.*, *op. cit.* note 80, p. 4.

¹¹⁶ Danish Draft §65a (1).

that the 'amendment will result in the protection of the physical characteristics of the performer or artist, including voice because the performance of a performer and an artist is inextricably linked to their voice and appearance.'¹¹⁷ As an example, 'a digitally generated imitation of an author's book reading'¹¹⁸ is mentioned. On the other hand, the Danish Government emphasises several times that only a digitally generated realistic imitation of either a performance of a literary or artistic work or an artistic presentation will be covered. As an example of excluded cases, the explanatory notes name a digitally generated television interview with a performer or the imitation of private individuals.¹¹⁹ This could suggest a limitation of the protection to the (artistic) performance, not the personal likeness or voice of the artist.

The Danish Government seems to believe that AI-generated imitation constitutes a copy and use (i.e., reproduction) of an artist's performance for which the current law offers no protection.¹²⁰ As the explanation was not clear, the Commission requested supplementary information. In their answer, the Danish Government further explained that the current AI technology provides the means to make a reproduction of an artist's performance without a fixation.¹²¹ However, an explanation of how synthetic imitation in deepfakes relates to a reproduction or fixation that violates the rights of performers is lacking.¹²²

This unsolved problem in copyright protection against deepfakes may be the cause of the inconsistencies identified by the Commission. In their comments, the Commission concludes that the Danish Draft needs to clarify the object of protection – i.e., which digital imitations of performances should be covered by § 65a – to be in accordance with the limitations of the EU directives on the rights of reproduction of performers. The term 'performance' is an autonomous notion of EU law and cannot be freely given a national interpretation that would include personal traits of a performer.¹²³

To conclude, § 65a of the Danish Draft pursues the goal of improving protection of performers from deepfake imitation. The intended measure will, however, remain ineffective if, in accordance with EU directives, only the artist's performance and not the imitation of personality traits is protected. Completely

¹¹⁷ *Ibid.*, p. 40f.

¹¹⁸ *Loc. cit.*

¹¹⁹ *Loc. cit.*

¹²⁰ See *Ibid.*, p. 21; EU Commission, *op. cit.* note 80, p. 3.

¹²¹ See answer of the Danish Government to question 4, EU Commission, *op. cit.* note 110, p. 2.

¹²² EU Commission, *op. cit.* note 80, p. 2.

¹²³ See *Ibid.*, p. 3f.

synthetic deepfakes cannot be treated as reproductions of a performance if they constitute something entirely new.

5.3.6. Compliance with EU law

Regarding § 65a of the Danish Draft, the Commission asked the Danish Government to consider the requirements and margin of discretion of applicable EU directives. This applies especially if existing terms of EU directives such as 'performers' or 'performance' may require a broader interpretation to achieve the aim of the Danish proposal. These terms have an autonomous notion of EU law and cannot take on a national meaning.

In this regard, the introduction of the terms 'artist', 'artistic' and 'presentation'¹²⁴ into the Danish Copyright Act seems unusual, notably because there is no corresponding legal definition in the Danish Draft. In the explanatory notes, the Danish Government clarifies that the addition aims to extend the protection of performances to presentations that are not performances of a copyright-protected work according to § 1 of the Danish Copyright Act.¹²⁵ 'Artistic presentations' should exclude athletic or sporting performances, as they are purely technical without an artistic or aesthetic character. 'Artist' includes *'actors, singers, musicians, dancers and other individuals who stage, perform, sing, recite, lecture, act or otherwise carry out artistic performances.'*¹²⁶ This extension of the notion of performers addresses the difficulty of performing artists to prove the originality of their performance. The explanatory notes themselves admit that it may prove difficult to assess what is to be considered an artistic performance or presentation and what not.

There is an obvious overlap between the meaning of 'artist' and 'performer'. The term 'artistic presentation' also seems to extend the current meaning of protected performances, rather than introducing a novel term. The Danish Government will have to adjust the text of the Draft before proceeding with the legislative process to avoid non-compliance with EU directives.¹²⁷

¹²⁴ See Danish Draft § 1 No. 2, p. 5-9.

¹²⁵ *Ibid.*, No. 26.

¹²⁶ *Ibid.*, p. 27.

¹²⁷ EU Commission, *op. cit.* note 80, p. 2f.

5.4. Inspiration for Europe?

The Danish Government has taken the first step toward regulating deepfakes in Denmark and perhaps also in the EU. Unlike mere principles, a written draft can enable in-depth discussion of a legal regulation. That can be seen in the reaction of Member States to Denmark promoting its draft as a template for the EU during the Danish Presidency in the Council of the EU in the second half of 2025. While the majority of the Member States endorsed the draft, others raised concerns linked to the production and dissemination of deepfakes beyond copyright law.¹²⁸ Nevertheless, the interest in the topic of deepfakes in the legislative corpus of the EU is apparent.¹²⁹

As the analysis of the draft has shown, the Danish Draft will still need to be revised before entering into force. It is open to question whether intellectual property law is the appropriate tool to achieve the intended protection. Moreover, the Commission identified conflicts with EU law in the current draft. Therefore, further research and discussion is needed to determine whether the problem of deepfakes involving the imitation of personal characteristics is truly best tackled in the field of copyright or whether other legal initiatives are better suited for the endeavour. The aim of the Danish Draft to tackle the protection of personal characteristics is well-intended. In jurisdictions such as Germany and Austria that, similarly to Denmark, partly rely on unwritten rules for the protection of personal traits, legal scholars also have advocated for a codification of these principles to strengthen legal certainty. In light of deepfakes, the ambition of the Danish Draft could serve as a model; the codification on the basis of copyright, on the other hand, should not.

6. CONCLUSION

Deepfakes pose a structural challenge to the protection of personal characteristics such as likeness and voice against unauthorised use. Surveying the ELVIS Act in Tennessee and the copyright-anchored Danish Draft in Denmark, both follow the approach of strengthening an IP-based right to one's personal characteristics. Whereas the codification of protection of voice, which was either non-existent (Tennessee) or uncoded (Denmark), amounts to a welcome establishment of legal certainty, the basis in copyright or copyright-like frameworks proves

¹²⁸ *Ibid.*, p. 2.

¹²⁹ See for example the engagement of the EU parliament in response to the Digital Omnibus: fn. 6.

disruptive to the current legal framework. Due to the economic orientation of copyright, the framework built to protect against deepfakes may paradoxically create an incentive to further AI-based dissemination of likeness and voice. Therefore, legislative initiatives should seek to create a more balanced approach to regulating deepfakes. Frameworks for the protection of personality rights could serve as a foundation on which to build. In the context of the EU, further research will be needed to explore the role of data protection for a coherent system. As a global phenomenon, deepfakes call for a sustainable European and global response. With the slow international process, a national response can be a trigger to move forward. Denmark's legislative proposal – while not perfect yet – offers inspiration for further initiatives.

REFERENCES

BOOKS AND ARTICLES

1. Appl, C., *Digitale Identität: Schutz und Verwertung der Persönlichkeit im virtuellen Raum* in C. Appl; O. Kreutz (eds), *Daten Information Recht: Festschrift für Andreas Wiebe zum 65. Geburtstag*, Wien 2024.
2. Beverley-Smith, H.; Ohly, A.; Lucas-Schloetter, A., *Privacy, Property and Personality*, Cambridge University Press 2009.
3. Buchner, W., *Das Persönlichkeitsrecht des Abgebildeten* in Dittrich, R. (ed), *Festschrift 50 Jahre Urheberrechtsgesetz*, Manz 1986.
4. Christoff, A.T., *Long Live the King: The Influence of Elvis Presley on the Right of Publicity in Tennessee*, U. Mem. L. Rev., 41/2011, 667-699.
5. Ciresa, M., § 75 UrhG in Ciresa, M. (ed), *Österreichisches Urheberrecht*, Wien 2015.
6. Dokalik, D.; Mokrejs-Weinhappel, C.; Kathrein, G. (eds), *Das Große ABGB*, 38th edn, 2025.
7. Engel-Bunsas, C., *Das Recht an der eigenen Stimme*, Tectum Verlag, 2025.
8. Engel-Bunsas, C.; Lampmann, A., *Recht an der Stimme: ein Normierungsausschuss aus der Praxis*, GRUR-Prax 2025, 532–536.
9. EPRS, *Tackling deepfakes in European policy: Study*, 2021.
10. Fowler, S.L.; Fowler, J.D., *Why Tennessee's ELVIS Act Is the King of Artificial Intelligence Protections*, Vand. J. Ent. & Tech. L., 27(2)/2025, 259–278.
11. Frey, D.; Westphal, L., *Rechtlicher Schutz und Verwertung der Stimme als Persönlichkeitsmerkmal: Neue Herausforderungen durch Voice-Cloning-Technologien*, MMR 2025, 779–785.

12. Gomille, C., *Deepfakes und das allgemeine Persönlichkeitsrecht: Der Schutz von Stimme, Bildnis und Selbstdarstellung*, ZUM 2025, 500–509.
13. Hense, P.; Kahl, J.; Manthey, G.; Wagner, D., *Rechtsgutachten Netflix AI Training: im Auftrag von Verband Deutscher Sprecher:innen e.V.*, 2026.
14. Kokalari, A.; McNamara, M., *Amendments 171-317: Draft Report on the Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)*, (COM(2025)0836 – C10-0304/2025 – 2025/0359(COD)), 14 February 2026 2025/0359(COD).
15. Koziol, H.; Warzilek, A., *Der Schutz der Persönlichkeitsrechte gegenüber Massenmedien in Österreich* in Koziol, H.; Warzilek, A.; Aebi-Müller, R.E. (eds), *Persönlichkeitsschutz gegenüber Massenmedien*, Wien[ua] 2005.
16. Loewenheim, U. (ed), *Handbuch des Urheberrechts*, C.H. Beck 2021.
17. Meissel, F.-S., § 16 ABGB in Fenyves, A.; Kerschner, F.; Vonkilch, A. (eds), *Großkommentar zum ABGB - Klang-Kommentar: §§ 1 - 43 ABGB, Methodenlehre und Personenrecht*, Wien 2014.
18. Mitzscherlich, J., *Das Recht an der eigenen Stimme – Teil 2: Schutz vor ungewollter Kommerzialisierung und KI-Imitation*, AfP 2025, 475–484.
19. Moldawer, M., *ELVIS Act: From Authorship to Ownership in Intellectual Property Law*, Texas Intellectual Property Law Journal 2024, 19–66.
20. Moos, K., *My Body, My Voice: Defining Vocal Identity Rights to combat AI-Generated Deception*, Marq. Intell. Prop. & Innovation L. Rev., 29(2)/2025, 350–362.
21. Pérez, G.E.M.; Castro, L.H., *Copyright or personality rights? A critical analysis of Denmark's approach to deepfakes*, IDP Revista de Internet, Derecho y Política 2026, 1-14.
22. Pierer, J., *Künstliche Intelligenz und Persönlichkeitsrecht: Mit Bewährtem gegen Neues*, ecolex 2024, 752–755.
23. Preminger, A.; Kugler, M., *The Right of Publicity Can Save Actors From Deepfake Armageddon*, BTLJ, 39/ 2023, 782–840.
24. Rothman, J., *The Right of Publicity: Privacy Reimagined for a Public World*, Harvard University Press 2018.
25. Thurner, A., *Bildmanipulation und Persönlichkeitsschutz in Zeiten von „Deepfakes“*, MR, 4/2019, 155–163.
26. Van der Sloot, B., *Regulating the synthetic society: Generative AI, Legal Questions and Societal Challenges*, Bloomsbury Publishing 2024.
27. Wendehorst, C., *Datenschutz im Zeitalter von KI: Wissenschaftlicher Diskussionsentwurf für eine neue „KI-Datenschutz-VO“ (Teil 2)*, KIR 2025, 174–182.

28. Westerlund, M., *The Emergence of Deepfake Technology: A Review*, TIM Review, 11/2019, 39–52.
29. Wiedemann, M.-J.; Stocks, F., *Der Klang der Zukunft: Die Auswirkungen der KI auf die Musikindustrie*, GRUR 2025, 360–364.
30. Zurth, P., *Deepfakes im Kontext des Urheber- und Leistungsschutzrechts*, ZUM 2025, 509–515.

LEGAL RULES

1. Berne Convention for the Protection of Literary and Artistic Works, September 9, 1886, as revised at Paris, July 24, 1971, and amended in 1979.
2. California Civil Code.
3. Ensuring Likeness Voice and Image Security Act - Tennessee Senate Bill 2096 (112th General Assembly), 07 March 2024.
4. EU Commission, *Issue of comments pursuant to Article 5(2) of Directive (EU) 2015/1535 of 9 September 2015 - Notification 2025/0654/DK - Act amending the Copyright Act (Introduction of performance protection and protection against digitally generated imitations, etc.)*, C(2026) 756 final, 2026.
5. New York Laws Civil Rights. L (Consol. 20239).
6. Tennessean Code Annotated.

COURT PRACTICE

1. Hart v. Elec. Arts, Inc. 717 F.3d 141, 147 (3th Cir. 2013).
2. Memphis Dev. Found. v. Factors, Etc. Inc. 441 F. Supp. 1323, 1330 (W.D. Tenn. 1977).
3. Midler v. Ford Motor Co., 849 F.2d 460 (9th Cir. 1988).
4. State ex rel. Elvis Presley Int'l Mem. Found. v. Crowell, 733 S.W.2d 89, 95 (Tenn. Ct. App. 1987).
5. White v. Samsung Electronics America Inc., 971 F.2d 1395, 1401 (9th Cir. 1992).
6. Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 573 (1977).

ONLINE SOURCES

1. Barnes, B; Sperling, N., Hollywood Actors Join Writers on Strike, Bringing Industry to a Standstill, The New York Times. 13 July 2023,

- <https://www.nytimes.com/2023/07/13/business/media/sag-aftra-writers-strike.html>, 26 March 2026.
2. Bekommt der Pumuckl wieder die Hans-Clarin-Stimme?, OVB Heimatzeitungen. 31 May 2022, <https://www.ovb-heimatzeitungen.de/rosenheim-region/2022/03/30/bekommt-der-pumuckl-wieder-die-hans-clarin-stimme.ovb?shorten>, 26 March 2026.
3. Conger, K.; Stuart, A., Elon Musk's Grok A.I. Chatbot Made Millions of Sexualized Images, New Estimates Show, The New York Times. 22 January 2026, <https://www.nytimes.com/2026/01/22/technology/grok-x-ai-elon-musk-deepfakes.html>, 26 March 2026.
4. Danish Government, *Draft of the Act amending the Copyright Act (Introduction of performance protection and protection against digitally generated imitations, etc.) Notification Detail*, 22 February 2026, <https://technical-regulation-information-system.ec.europa.eu/en/notification/27420>, 26 March 2026.
5. Deepttrace, The state of deepfakes: Landscape, threats, and impact, 2019, https://regmedia.co.uk/2019/10/08/deepfake_report.pdf, 26 March 2026.
6. ELI, *Simpler, Fairer, More Effective – Towards a Targeted Revision of EU Data Protection law: Feedback of the European Law Institute on the Digital Package – Digital Omnibus*, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_-_Simpler_fairer_more_effective.pdf, 26 March 2026.
7. EPRS, The Danish approach to copyright and deepfakes: A model for the EU?, January 2026, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782611/EPRS_ATA\(2026\)782611_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782611/EPRS_ATA(2026)782611_EN.pdf), 26 March 2026.
8. EU Commission, *Act amending the Copyright Act (Introduction of performance protection and protection against digitally generated imitations, etc.): Notification Detail*, 31 October 2025, <https://technical-regulation-information-system.ec.europa.eu/en/notification/27420>, 26 March 2026.
9. EU Commission, *Forwarding of the response of the Member State notifying a draft (Denmark) to request for supplementary information (INFOSUP) of European Commission (Message number 3402): Notification: 2025/0654/DK*, 28 November 2025, <https://technical-regulation-information-system.ec.europa.eu/en/notification/27420>, 26 March 2026.
10. Kulturministeriet, Bred aftale om deepfakes giver alle ret til egen krop og egen stemme, 06 June 2025, <https://kum.dk/aktuelt/nyheder/bred-aftale-om-deepfakes-giver-alle-ret-til-egen-krop-og-egen-stemme>, 26 March 2026.
11. Kulturministeriet, Deepfakes, produktionsrabat og mindre bureaukrati er på årets lovprogram, 07 October 2025,

- <https://kum.dk/aktuelt/nyheder/deepfakes-produktionsrabat-og-mindre-bureaukrati-er-paa-aarets-lovprogram.>, 26 March 2026
12. Kulturministeriet, Værn mod deling af digitale efterligninger af personlige kendetegn, 26 June 2025, https://kum.dk/fileadmin/_kum/1_Nyheder_og_presse/2025/Vaern_mod_deling_af_digiale_efterligninger.pdf, 26 March 2026.
 13. Microsoft Research, VALL-E, 09 May 2025, <https://www.microsoft.com/en-us/research/project/vall-e-x/>, 26 March 2026.
 14. Rbb, J.S., Streit mit Netflix: Synchronsprecher protestieren gegen KI-Klausel, tagesschau.de, 8 February 2026, <https://www.tagesschau.de/wirtschaft/synchronsprecher-netflix-ki-100.html>, 26 March 2026.
 15. Salnikow, A., Term deepfakes in Art. 3 No. 3 of the AI Act in different languages - overview, <https://lush-antelope-62c.notion.site/Term-deepfakes-in-Art-3-No-3-of-the-AI-Act-in-different-languages-overview-315909c4539280199771d169c2f7368c>, 26 March 2026.
 16. This Person Does Not Exist - Random Face Generator. 2021-2023, <https://this-person-does-not-exist.com/en>, 26 March 2026.
 17. Waybackmachine, Webpage of the Reddit user 'deepfakes' on 17 December 2017, <https://web.archive.org/web/20171212214356/https://www.reddit.com/user/deepfakes/submitted/>, 26 March 2026.
 18. Weitzman, C., Voicify AI: Revolutionize Your Voice Content Creation, Speechify, 2025, https://speechify.com/blog/voicify-ai/?srsltid=AfmBOopNiUWFuwKT48azT29mK0DEuXIkmt7GY-JEIV4EJqFgiphr_k_, 26 March 2026.

UDK: 343.541-053.2 : 004.738.5 (4-67 EU)
Preliminary communication

Dóra Rengel, PhD student
Faculty of Law, University of Pécs, Hungary
E-mail: rengel.dora@ajk.pte.hu
ORCID-ID: 0009-0001-9477-9726

THE EU REGULATORY FRAMEWORK ON DEEPFAKE CHILD SEXUAL ABUSE MATERIAL: CURRENT SOLUTIONS AND FUTURE DIRECTIONS

ABSTRACT

This study examines the European Union's regulatory framework governing synthetic content depicting the sexual abuse of children created through deepfake technology (AI-generated CSAM). Advances in artificial intelligence now enable the production of highly realistic imagery that may not be linked to an identifiable victim, yet still constitutes a serious infringement of children's sexual integrity. The analysis demonstrates that although the Digital Services Act and the AI Act introduce important platform-governance and transparency obligations, neither instrument provides a comprehensive response to the challenges posed by AI-generated CSAM. The current conceptual framework of Directive 2011/93/EU likewise struggles to address fully synthetic material. The Recast Directive represents a significant step forward by explicitly extending the definition of CSAM to include deepfake recordings and realistic digital representations. In parallel, the proposed CSAR would impose mandatory risk-assessment and detection obligations on service providers; however, this raises substantial EU fundamental-rights concerns, particularly regarding data protection and the right to privacy. The study concludes that an effective response to deepfake child sexual abuse material requires coordinated criminal-law, platform-regulation and AI-governance mechanisms. Such a framework can only be realised through sustained cooperation between legislators, technology developers, service providers and civil-society actors.

Keywords: *deepfake, AI-generated child sexual abuse material, AI Act, DSA, future EU regulatory framework*

1. INTRODUCTION

The development of artificial intelligence-based image-generation and image-manipulation technologies has created new challenges in the field of cybercrime. Deepfake technology enables the production of visual and audiovisual content that creates the appearance of reality while depicting individuals or events that do not in fact exist. One of the most severe manifestations of this phenomenon is the

artificial creation of sexualised depictions of children (hereinafter: AI-generated CSAM). These technologies are evolving more rapidly than the law can follow, creating an urgent need for legislative frameworks that provide modern, deepfake-specific solutions.¹

The European Union (hereinafter: EU) has recently introduced comprehensive reforms to regulate the digital environment, most notably through the adoption of Regulation (EU) 2022/2065 of the European Parliament and of the Council on digital services and amending Directive 2000/31/EC (hereinafter: Digital Services Act, DSA), and Regulation (EU) 2024/1689 of the European Parliament and of the Council on artificial intelligence and amending certain Union legislative acts (hereinafter: AI Act). The core criminal-law framework related to child sexual abuse material remains defined by Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, replacing Council Framework Decision 2004/68/JHA (hereinafter: Directive 2011/93/EU). However, deepfake child pornography challenges both the effectiveness and internal coherence of these norms.

A central question is how AI-generated content—whether fully synthetic or created using the facial features or body parts of real children—fits within the EU’s conceptual framework on child pornography. At the same time, it must be examined whether the regulatory model grounds protection exclusively in the concrete child victim, or whether it also recognises an abstract legal interest in safeguarding children’s sexual integrity more broadly. From a practical perspective, further questions arise as to whether the new rules applicable to online platforms and to artificial intelligence systems are capable of ensuring the effective prevention and removal of such content.

The proposed recast of Directive 2011/93/EU (hereinafter: Recast Directive) and the draft EU Regulation laying down rules to prevent and combat child sexual abuse—known as the Child Sexual Abuse Regulation or “Chat Control” (hereinafter: CSAR)—are still pending at Union level. The CSAR proposal, however, raises significant fundamental rights concerns, particularly regarding the rights to respect for private and family life and to the protection of personal data,

¹ Zverev, V., Bushkov, V., Khrushkov, B., Sarychev, V., Ostaltsev, O., & Prokopovych-Tkachenko, Y., *Artificial intelligence and cybercrime: New challenges and prospects for legal regulation*, Contemporary Issues in Artificial Intelligence, 1/2025, p. 2.

as guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.²

The key issue, therefore, is whether the EU regulatory framework can effectively counter deepfake child pornography without infringing fundamental rights—most notably the principles of necessity and proportionality. The aim of this study is to provide a systematic analysis of the EU legal framework governing deepfake child sexual abuse material, to identify conceptual and structural uncertainties, and, where appropriate, to formulate *de lege ferenda* recommendations. The analysis proceeds from the assumption that while the current normative toolbox is, in principle, capable of addressing the phenomenon, clarification of conceptual boundaries is essential to ensure legal certainty.

The research primarily employs a doctrinal legal methodology, focusing on the definitions of deepfake technology and child pornography in EU law and on the interpretation of the normative content of relevant legal sources. The study also takes account of the current state of ongoing legislative processes. The first part introduces the EU definitions of deepfake technology and child pornography and explains the social relevance and prevalence of the phenomenon, supported by statistical data. This is followed by an analysis of the relevant EU regulatory frameworks—particularly the DSA, the AI Act, Directive 2011/93/EU, the Recast Directive and the CSAR. The concluding part emphasises that combating deepfake child sexual abuse material requires a complex, multi-level approach in which legislation, law enforcement, and technological solutions play equally essential and mutually reinforcing roles.

2. CONCEPTUAL FOUNDATIONS

2.1. Deepfake

2.1.1. The concept and origin of deepfakes

The complexity of the subject matter requires a clear clarification of the conceptual foundations. This chapter therefore begins with the definition of “deepfake.” In EU law, the term receives an explicit normative definition in the text of the AI Act. Pursuant to Article 3(60) of the Regulation, a deepfake is any AI-generated or

² Charter of Fundamental Rights of the European Union, Articles 7 and 8, ^[1]^[2]Official Journal of the European Union, C 326, 26.10.2012, pp. 391–407 (hereinafter: EU Charter)

AI-manipulated image, audio or video content that resembles existing persons, objects, places, entities or events, and that may appear authentic or real to a natural person in a misleading manner.³

Nevertheless, the term "deepfake" stems from the combination of "deep learning" and "fake."⁴ The phenomenon emerged in 2017 and represents a new form of artificially produced synthetic media.⁵ For a broader conceptualisation, a more comprehensive, synthesised definition is appropriate—one that draws on multiple definitional approaches. Deepfakes constitute digital media manipulation,⁶ a dangerous form of visual disinformation,⁷ generated using artificial intelligence and deep learning techniques.⁸ As a result, they produce falsified content⁹ that convincingly creates the impression that both the content and its depicted subjects are real and authentic, while they are in fact fully manipulated.¹⁰

In the context of the present study, deepfake technology appears in two principal forms.¹¹ First, existing visual material may be manipulated. In such cases, the facial features or body parts of a real child may be inserted into other—potentially sexually explicit—recordings, or the context of originally non-sexual material may be altered. Thus, offenders may employ artificial intelligence to modify an image of a child to make it appear as if the child were unclothed or depicted in illegal content, or to rework, extend, or reframe previously unlawful recordings, thereby

³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), Article 3(60), Official Journal of the European Union, L 2024/1689, 12.7.2024 (hereinafter: AI Act)

⁴ Kietzmann, J.; Lee, L. W.; McCarthy, I. P.; Kietzmann, T. C., *Deepfakes: Trick or Treat*, Business Horizons, year 63, 2/2019, pp. 135–146.

⁵ Sandoval, M.-P.; de Almeida Vau, M.; Solaas, J.; Rodrigues, L., *Threat of deepfakes to the criminal justice system: a systematic review*, Crime Science, year 13, 1/2024, p. 1.

⁶ Veszelszki, Á., *Deepfake: kételkedés a kételyben*, In: Aczél, P.; Veszelszki, Á. (eds.), *Deepfake: a valótlan valóság*, Gondolat Kiadó, Budapest, 2023, p. 15.

⁷ Weikmann, T.; Greber, H.; Nikolaou, A.; *After Deception: How Falling for a Deepfake Affects the Way We See, Hear, and Experience Media*, The International Journal of Press/Politics, 1/2025, p. 104.

⁸ Whittaker, L.; Mulcahy, R.; Letheren, K.; Kietzmann, J.; Russell, R.; Bennett, B.; *Mapping the deepfake landscape for innovation: A multidisciplinary systematic review and future research agenda*, Technovation, 1/2023, p. 23.

⁹ Temir, E.; *Deepfake: New Era in The Age of Disinformation & End of Reliable Journalism*, Selçuk İletişim Dergisi, 2/2020, p. 1012.

¹⁰ Lendvai, G. F.; *Deepfake a szólásszabadság tükrében – reflexiók a jog perspektívájából*, Gondolat Kiadó, Budapest, 2023, p. 122.

¹¹ Ganesh, H. K.; *Protecting Children Through Deepfake Child Pornography: A Moral, Legal, and Philosophical Discussion on the Intersection of the Evolution in Law and Technology*, American Criminal Law Review, 60/2022, p. 7.

creating additional victimisation for individuals already depicted.¹² Second, fully synthetic content may be produced, whereby AI systems generate realistic but non-existent individuals and scenes based on textual instructions (prompts).¹³ Despite their synthetic nature, such visual material can equally reinforce patterns that normalise abusive behaviour and may contribute to encouraging offences against real victims.¹⁴

2.1.2. Technological characteristics of deepfakes

2.1.2.1. Generative Adversarial Networks (GANs)

Understanding how manipulated content is constructed is essential; therefore, the underlying technological approaches—typically three major categories—require explanation. GANs constitute one of the most commonly used foundations of deepfake technology. They consist of two competing neural networks: the generator, which produces new, falsified images or videos, and the discriminator, which aims to distinguish the generator's output from real material. Through this "competition," both networks undergo continuous optimisation,¹⁵ contributing to increasingly convincing results.¹⁶

2.1.2.2. Autoencoders and Variational Autoencoders (VAEs)

An autoencoder consists of three components: an encoder that extracts key features from images—such as skin tone, facial expression or eye position—and compresses them; a latent space in which these features are stored; and a decoder that reconstructs the image from the latent representation. In deepfake

¹² U.S. Department of Homeland Security – Homeland Security Investigations, *Artificial Intelligence and Combating Online Child Sexual Exploitation and Abuse*, Know2Protect campaign, online infographic, https://www.dhs.gov/sites/default/files/2024-09/24_0920_k2p_genai-bulletin.pdf, 3 January, 2026.

¹³ Internet Watch Foundation (IWF), *How AI is being abused to create child sexual abuse imagery, institutional report*, October 2023, p. 6, https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf, 18 January, 2026.

¹⁴ Dushi, D.; Berdufi, N.; Karagianni, A., *The legal framework and legal gaps for AI-generated child sexual abuse material*, Computer Law & Security Review, 59/2025, p. 1.

¹⁵ Luan, T., *A Survey on Deepfake Detection Technologies*, International Journal of Emerging Technologies and Advanced Applications, 2/2025, p. 2.

¹⁶ Zhang, T., *Deepfake generation and detection, a survey*, Multimedia Tools and Applications, 81/2022, p. 6261.

face-swapping, two separate decoders are trained for two different faces, while a single shared encoder processes both. Thus, the face of Person A can be replaced with that of Person B by encoding A's image and decoding it with B's decoder. The resulting image shows Person B's face on Person A's body.¹⁷ Variational autoencoders differ somewhat, as they model the latent space statistically. While traditional autoencoders compress and reconstruct images in a fixed manner, VAEs encode inputs as probability distributions (mean and variance) within the latent space. The decoder then reconstructs images through sampling from these distributions, making it possible to generate multiple variations from a single input.¹⁸

2.1.2.3. Diffusion Models

In machine learning, diffusion models generate new data—such as images—by progressively adding noise to the training data and then learning to reconstruct the original data by reversing the noise-adding process.¹⁹ First, a neural network is trained to corrupt images with noise, as if making them increasingly blurred. The system then learns how to remove the noise, producing clean, high-fidelity images that resemble the originals. Technologies such as DALL·E 2, Midjourney and Stable Diffusion rely on this approach and can generate highly realistic images based solely on textual prompts.²⁰

2.2. Child Sexual Abuse Material

For assessing AI-generated child sexual abuse material within the EU legal framework, the point of departure is the definition in Article 2(c) of Directive 2011/93/EU. Before defining the term, the Directive clarifies that a “child” means

¹⁷ Patel, Y.; Tanwar, S.; Gupta, R.; Bhattacharya, P.; Davidson, I. E.; Nyameko, R.; Aluvala, S.; Vimal, V., *Deepfake Generation and Detection: Case Study and Challenges*, IEEE Access, 11/2023, p.143301.

¹⁸ Choudhary, A. S., *What is Variational Autoencoders?* Data Science Blogathon 2025, <https://www.analyticsvidhya.com/blog/2023/07/an-overview-of-variational-autoencoders/>, 22 April, 2025.

¹⁹ O'Connor, R., *Introduction to Diffusion Models for Machine Learning*, Assemblyai 2022, <https://www.assemblyai.com/blog/diffusion-models-for-machine-learning-introduction#:~:text=Let's%20dive%20in!,Diffusion%20Models%20%2D%20Introduction,through%20the%20learned%20denoising%20process>, 30 June, 2025.

²⁰ *Introduction to diffusion models for machine learning*. Superannotate 2025, <https://www.superannotate.com/blog/diffusion-models#:~:text=Diffusion%20models%20are%20prominent%20in,distribution%20from%20the%20noisy%20data>, 25 June, 2025.

any person below the age of 18 (Article 2(a)).²¹ Additionally, Article 2(b) introduces the concept of the "age of consent," referring to the age below which any sexual activity with a child is prohibited under national law.²²

The Directive's preamble emphasises the need for clarity regarding what constitutes child pornography under EU law.²³ This is crucial because such material can take numerous forms (real, simulated, realistic, depictions of persons appearing as children, etc.), and effective law enforcement requires a precise definition that covers all relevant conduct. The Directive therefore adopts a broad definition encompassing several partially distinct, partially overlapping categories.

Under point (i), child pornography includes any material that visually depicts a child engaged in real or simulated explicit sexual conduct. This category traditionally concerns recordings involving actual, identifiable children.

Point (ii) widens the scope further by independently criminalising depictions of the sexualised display of a child's sexual organs, irrespective of whether explicit conduct occurs.

Point (iii) directly addresses challenges arising from technological developments by covering material depicting a person appearing to be a child engaged in explicit sexual conduct, or the sexualised display of such a person's sexual organs.

Point (iv) adds further nuance by expressly including "realistic images" of children engaged in explicit sexual conduct or realistic images of a child's sexual organs when produced primarily for sexual purposes.²⁴

Thus, EU law adopts a broad protective approach that criminalises not only depictions involving real children, but also virtual child pornography (digitally generated content that creates sexualised depictions of child-like figures without involving real children)²⁵ and pseudo-child pornography (digitally altered content using body parts or facial features of real individuals to create material that appears

²¹ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, OJ L 335, 17.12.2011 (hereinafter: Directive 2011/93/EU), Article 2(a).

²² Directive 2011/93/EU, Article 2(b).

²³ Directive 2011/93/EU, Preamble (12).

²⁴ Directive 2011/93/EU, Article 2(c).

²⁵ Burke, D. D.; Doval, C. N., *Redefining child pornography in an age of technological advancement: The concept of avoidable harm*, Washington Journal of Law, Technology & Arts, year 20, 3/2025, p. 49.

to depict a child, without involving an actual minor).²⁶ This approach allows deepfake-generated content to fall within the definition of child pornography where it meets the criteria of "a person appearing to be a child" or "realistic images." Nonetheless, conceptual uncertainties arise—particularly concerning the category of "realistic images."²⁷ The proposed Recast Directive may introduce relevant modifications to these definitions, should the draft be adopted. These potential changes will be discussed later in this study.

The current framework leaves certain discretion to Member States. They may, for example, decide whether to criminalise material falling under point (iii) where the individuals depicted are adults who are made to appear younger.²⁸ Member States may also choose whether to prohibit the creation or possession of "realistic" images under point (iv) when such content is created and held exclusively for private use, is purely fictional, does not involve real children, and presents no risk of dissemination.²⁹

Article 8(3) further expands this discretion by allowing Member States to decide whether criminal sanctions apply in cases where:

- the persons depicted are minors who have reached the age of consent,
- the material was produced and is possessed with their mutual consent,
- and no coercion, abuse or exploitation occurred.³⁰

3. STATISTICAL DIMENSIONS OF THE DEEPFAKE PHENOMENON

The social harmfulness of the deepfake phenomenon is unequivocally supported by empirical data. The spread of the technology has been extraordinarily rapid: while an estimated 500,000 deepfake items were accessible online in 2023, projections indicated that by 2025 this number would exceed 8 million. This represents an increase of more than 1,500% within two years,³¹ with the volume

²⁶ Negredo, L.; Herrero, Ó., *Child pornography on the Internet*, Papeles del Psicólogo / Psychologist Papers, year 37, 3/2016, p. 218.

²⁷ Rigotti, C.; Gkioka, C. P.; Do Rosario Da Graça, S.; Lannier, S., *Overlapping offences, divergent logics: Reconciling EU law on sexual imagery of minors*, New Journal of European Criminal Law, 2025, p. 17.

²⁸ Directive 2011/93/EU, Article 5(7).

²⁹ Directive 2011/93/EU, Article 5(8).

³⁰ Directive 2011/93/EU, Article 8(3).

³¹ European Parliament, *Children and deepfakes*, Briefing, European Parliamentary Research Service (EPRS), 2025, 2025, p. 2,

of such content doubling approximately every six months. The phenomenon is therefore not merely expanding, but doing so at an exponential pace.³²

However, the problem is not solely quantitative. According to estimates by the European Commission, approximately 98% of deepfake content is pornographic in nature,³³ indicating that current patterns of technological use are predominantly shifting toward sexual exploitation. Europol's forecasts reinforce the seriousness of these trends: by 2026, up to 90% of online content may be synthetically generated, fundamentally challenging the credibility of digital material and the ability to distinguish between reality and manipulation. Within the category of sexual deepfakes, the proportion involving minors is particularly alarming. Studies indicate that one in seven internet users has encountered a sexual deepfake, while approximately 17% of artificially generated sexualised content involves minors.³⁴ The large-scale emergence of AI-generated child sexual abuse material (AI-CSAM) has become one of the most severe online safety trends within the European Union.³⁵ International data from 2024 show that 90% of such material reaches a level of realism that may render it equivalent, from a legal-assessment perspective, to recordings involving real children. Reports related to AI-CSAM increased from 4,700 in 2023 to 67,000 in 2024—a 1,325% rise—most of which exhibited a clear European nexus.³⁶

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf), 12 February, 2026.

³² Sensity, *How to Detect a Deepfake Online: Image Forensics and Analysis of Deepfake Videos*, 2021, <https://sensity.ai/blog/how-to-detect-a-deepfake/>, 24 June, 2025.

³³ Furizal; Ma'arif, A.; Maghfiroh, H.; Suwarno, I.; Prayogi, D.; Kariyamin; Lonang, S.; Sharkawy, A.-N., *Social, legal, and ethical implications of AI-generated deepfake pornography on digital platforms: A systematic literature review*, Social Sciences & Humanities Open, Year 12, 2025, p. 13.

³⁴ European Parliament, *Children and deepfakes*, mBriefing, European Parliamentary Research Service (EPRS), 2025, p. 2-3, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf), 12 February, 2026.

³⁵ Internet Watch Foundation (IWF), *What has changed in the AI CSAM landscape?*, AI CSAM Report Update, Version 1.1, July 2024, p. 25, https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf, 5 January, 2026.

³⁶ European Parliament, *Combating child sexual abuse online*, Briefing – EU Legislation in Progress, European Parliamentary Research Service (EPRS), 2025, p. 1, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI\(2022\)738224_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf), 29 January, 2026.

4. EU THE EU'S EXISTING NORMATIVE FRAMEWORK

4.1. DSA

4.1.1. Illegal Content from the Perspective of the DSA

Following the risk assessment of deepfakes, this section examines how the European Union's current regulatory framework—most notably the DSA, which partly replaces the previously inconsistent and divergent self-regulatory practices of digital platforms—responds to this phenomenon.³⁷ The DSA seeks to more effectively tackle illegal content disseminated via online intermediary services and to provide stronger user protection, while balancing the fundamental rights of both service providers and users.³⁸

Although the DSA does not contain explicit provisions concerning deepfake child sexual abuse material, child sexual abuse material (CSAM) unequivocally falls within the Regulation's category of "illegal content."³⁹ Under the DSA, illegal content is defined broadly as any information that is unlawful under EU or national law.⁴⁰ Even though the domestic law of certain Member States does not yet expressly criminalise AI-generated CSAM, such material remains illegal under EU law based on the definitional framework of Directive 2011/93/EU. Accordingly, the DSA applies fully to AI-generated and manipulated CSAM. Article 7 of the DSA allows providers to voluntarily undertake investigations and implement measures aimed at the detection, identification and removal of illegal content.⁴¹ Under Article 16, hosting service providers must operate efficient notice-and-action mechanisms, enabling users to report illegal content in a straightforward and transparent manner.⁴² To support this, Article 12 requires providers to designate a single point of contact that ensures swift and direct

³⁷ Sorbán, K., *A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről*, *Belügyi Szemle*, 10/2020, p. 81.

³⁸ Wilman, Folkert, *The Digital Services Act (DSA) – An Overview, working paper*, European Commission, 2022, p. 1.

³⁹ Buri, I.; van Hoboken, J., *The Digital Services Act (DSA) proposal: a critical overview, Discussion paper, Digital Services Act (DSA) Observatory*, Institute for Information Law (IViR), University of Amsterdam, 2021, p. 8.

⁴⁰ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (hereinafter: DSA), Article 3(h)

⁴¹ European Data Protection Board (EDPB), *Guidelines 3/2025 on the interplay between the Digital Services Act and the GDPR*, 2025, p. 9-10, https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202503_interplay-dsa-gdpr_v1_en.pdf, 10 December, 2025.

⁴² DSA, Art. 16(1)–(2)

electronic communication with users and competent authorities.⁴³ Platforms must act without undue delay, inform the notifier of the decision taken, and provide access to redress mechanisms.⁴⁴

The DSA establishes differentiated obligations based on the size and societal impact of platforms. Digital service providers fall into four categories: intermediary services, hosting services, online platforms and very large online platforms and search engines (VLOPs and VLOSEs).⁴⁵ Very large platforms and search engines with more than 45 million EU users⁴⁶ (such as AliExpress International (Netherlands) B.V., Amazon EU S.à.r.l., Google Ireland Ltd.)⁴⁷ are subject to extensive risk-management obligations. The Commission has designated 17 platforms as VLOPs and 2 services as VLOSEs.⁴⁸ Under Article 35, these providers must identify and assess systemic risks—including the dissemination of illegal content such as CSAM and AI-generated CSAM⁴⁹—and develop reasonable and effective mitigation measures.⁵⁰

Such measures may include modifications to user interfaces, revisions of terms of service, improvements in notice-and-action processes, adjustments to algorithmic systems, enhanced visibility of reliable information, labelling of suspicious content, and the adoption of codes of conduct.⁵¹

Action against illegal content is ensured through cooperation with national authorities; accordingly, Articles 9 and 10 of the DSA allow for specific removal or data-disclosure orders, while continuing to prohibit any general monitoring obligation.⁵² The DSA further dedicates a separate chapter to the online protection

⁴³ Gsell, Florence; *The Digital Services Act (DSA): A General Assessment*, In: von Ungern-Sternberg, Antje (ed.), *Content Regulation in the European Union – The Digital Services Act*, TRIER Studies on Digital Law, year 1, Verein für Recht und Digitalisierung e.V., Institute for Digital Law (IRDT), Trier, 2023, p. 9.

⁴⁴ DSA, Art. 16 (5)

⁴⁵ Genç-Geleç, B., *Regulating digital platforms: Will the DSA correct its predecessor's deficiencies?*, Croatian Yearbook of European Law and Policy, year 18, 2022, p. 59.

⁴⁶ DSA, Art. 33(1)

⁴⁷ European Commission, *Supervision of the designated very large online platforms and search engines under the Digital Services Act*, <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>, 10 February, 2026.

⁴⁸ European Commission, *The enforcement framework under the Digital Services Act*, <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement>, 19 February, 2026.

⁴⁹ Parti, K.; Szabó, J.; *The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe*, Laws, year 13, 6/2024, p. 3,

⁵⁰ DSA, Art. 33-35.

⁵¹ Gsell, *op. cit.*, note 43, p. 16.

⁵² Gsell, *op. cit.*, note 43, p. 10.

of minors. Article 28 mandates service providers accessible to minors to adopt measures ensuring a high level of privacy, safety and protection.⁵³ Additionally, targeted advertisements based on profiling using minors' personal data—within the meaning of the GDPR—are strictly prohibited where the provider can reasonably determine that the user is a minor.⁵⁴

The DSA's enforcement architecture operates through a dual structure: national Digital Services Coordinators supervise compliance at Member State level, whereas the European Commission exercises exclusive oversight over very large platforms.⁵⁵ The Commission may launch investigations, request information and conduct on-site inspections.⁵⁶ Non-compliant very large platforms may face fines of up to 6% of their global annual turnover. Since the Regulation's entry into force, several high-profile investigations have been initiated, including against TikTok for a potentially addictive reward system, and against AliExpress for the dissemination of illegal products.⁵⁷ Major platforms—such as TikTok and Facebook—have introduced specialised training for content moderators to improve their ability to identify and address illegal material, including CSAM.⁵⁸

4.1.2. Practical Enforcement of the DSA and the Lessons of the Grok Scandal

The January 2026 Grok scandal highlighted the risks involved. The Grok chatbot developed by xAI was capable of generating sexually explicit synthetic images of minors through the digital removal of clothing, producing approximately 6,700 such images within two days. Although xAI quickly introduced restrictions, the EU launched an investigation to determine whether the platform had violated the DSA provisions on combating illegal content.

The Commission had already imposed a €120 million fine on X for earlier transparency infringements and ordered the preservation of all data related to

⁵³ Wilman, Folkert, *The Digital Services Act (DSA) – An Overview, working paper*, European Commission, 2022, p. 11.

⁵⁴ DSA, Art. 28(2)

⁵⁵ European Commission, *The Digital Services Act*, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>, 8 October, 2025.

⁵⁶ European Commission, *The enforcement framework under the Digital Services Act*, <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement>, 19 February, 2026.

⁵⁷ European Commission, *Digital Services Act: keeping us safe online*, 2025, https://commission.europa.eu/news-and-media/news/digital-services-act-keeping-us-safe-online-2025-09-22_en, 19 December, 2025.

⁵⁸ European Parliament, *Combating child sexual abuse online*, Briefing – EU Legislation in Progress, European Parliamentary Research Service (EPRS), 2025. p. 3, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI\(2022\)738224_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf), 29 January, 2026.

Grok's operation. In the wake of the scandal, several Members of the European Parliament called for a Union-wide ban on such systems, and an amendment to the AI Act was also discussed that would classify AI-generated sexual content involving children as an "unacceptable risk" practice.⁵⁹

4.2. AI Act

4.2.1. The Regulatory Architecture of the AI Act

The objective of the AI Act is to ensure that AI systems are developed and deployed in a manner that is safe and trustworthy for EU citizens, while supporting the emergence of a strong and competitive European AI ecosystem. The Regulation simultaneously protects individuals' safety and fundamental rights, enhances transparency and accountability, fosters innovation, and creates a stable and predictable market environment.⁶⁰

The Act is built upon a risk-based regulatory structure, classifying AI systems into four categories according to their potential risks: prohibited (unacceptable), high-risk, limited-risk and minimal-risk systems. Each category entails distinct compliance obligations and corresponding levels of oversight.⁶¹

The AI Act imposes a full ban from February 2025 on AI systems that pose unacceptable risks to individuals' safety or fundamental rights, including manipulative or exploitative practices, social scoring and certain intrusive biometric techniques.⁶² High-risk AI systems — such as those used in healthcare or the administration of justice — are subject to strict requirements, including risk management and human oversight. AI tools falling under transparency obligations, including those generating deepfake content, must ensure that such outputs are recognisable and appropriately labelled; these provisions will apply from August 2026.

⁵⁹ European Newsroom (ENR), *Nudification blocks: The EU's struggle for more safety online*, 2026, <https://europeannewsroom.com/nudification-blocks-the-eus-struggle-for-more-safety-online/>, 6 February, 2026.

⁶⁰ Kim, B.-J.; Jeong, S.; Cho, B.-K.; Chung, J.-B., *AI Governance in the Context of the EU AI Act*, IEEE Access, 2025, p. 144127.

⁶¹ Ducret, M.; Wahal, E.; Gruson, D.; Amrani, S.; Richert, R.; Mouncif MOUNGACHE, M.; Schwendicke, F., *Trustworthy Artificial Intelligence in Dentistry: Learnings from the EU AI Act*, Journal of Dental Research, year 103, 11/2024, p. 1052.

⁶² Boştân, I., *Consolidating the Role of AI in the Economy and Society: Combatting the Deepfake Phenomenon Through Strategic and Normative Approaches – The Case of Romania in the EU Context*, Economies, year 13, 5/2025, p. 12.

The regulation imposes no requirements on AI systems that present minimal or negligible risk, such as AI-enhanced video game features or spam filters.⁶³

Since the current risk categories are tied to the application domains of AI systems, there is a possibility that a system's actual risk level may be misjudged, potentially undermining the effective enforcement of the AI Act. This issue is particularly acute in the case of general-purpose AI (GPAI), which can be used in numerous, and often unpredictable, ways.⁶⁴

Moreover, the AI Act only partially addresses several risks associated with malicious AI use, which becomes especially evident in relation to severe abuses such as AI-generated child sexual abuse material. Although AI-generated CSAM does not appear as a separate category in Article 5, a potential link may arise under Article 5(1)(b).⁶⁵ This provision covers AI systems specifically designed or used to exploit the vulnerabilities of certain groups—such as children, who are inherently vulnerable due to their age. Nevertheless, the AI Act does not itself establish any dedicated prohibitions or obligations aimed at the prevention, detection or mitigation of AI-generated CSAM. The Act's transparency-based rules for identifying deepfake content can be easily circumvented and are insufficient for addressing the risks posed by AI-generated CSAM. Effective intervention therefore necessarily requires the combined application of multiple EU legal instruments specifically tailored to this domain.⁶⁶

In designing their risk-management systems, providers must pay particular attention to whether a high-risk AI system is accessible to children or likely to have an impact on them.⁶⁷ Due to children's heightened vulnerability and their distinct rights,⁶⁸ developers and operators of such systems must implement additional safeguards to ensure an appropriate level of protection.⁶⁹

⁶³ European Commission, *AI Act*, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>, 14 November, 2025.

⁶⁴ Novelli, C.; Casolari, F.; Rotolo, A.; Taddeo, M.; Floridi, L., *Taking AI risks seriously: a new assessment model for the AI Act*, AI & Society, year 39, 2024, p. 1.

⁶⁵ AI Act, Art. 5(1)(b)

⁶⁶ Elcano Royal Institute, *Risk without borders: the malicious use of AI and the EU AI Act's global reach*, Analysis, <https://www.realinstitutoelcano.org/en/analyses/risk-without-borders-the-malicious-use-of-ai-and-the-eu-ai-acts-global-reach/>, 10 February, 2026.

⁶⁷ Charisi, V.; Chaudron, S.; Di Gioia, R.; Vuorikari, R.; Escobar-Planas, M.; Sanchez, I.; Gomez, E., *Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy*, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, 2022, p. 21.

⁶⁸ AI Act, Recital (9)

⁶⁹ Schuett, J., *Risk Management in the Artificial Intelligence Act*, European Journal of Risk Regulation, year 15, 2/2023, p. 16-17.

Article 50 sets out transparency obligations for the creation, use and labelling of deepfakes and other forms of synthetic media. Under paragraph (4), any person who creates AI-manipulated image or audio content that appears realistic must disclose its artificial origin, except in cases of lawful use in criminal proceedings; for artistic or satirical content, a lighter form of labelling is permitted. Paragraph (2) further requires providers to ensure that generated content is labelled in a machine-readable, reliable and interoperable manner.⁷⁰ At present, however, no existing technology fully satisfies these requirements.⁷¹

4.2.2. Practical Labelling and Detection of Deepfake Content

Although the Regulation requires deepfake content to be labelled, it does not specify the precise technical form such labelling should take. The most common method is the use of digital watermarking. Digital watermarking is a technology that enables information related to intellectual property rights—such as the author's name, a logo or a serial number—to be embedded into multimedia content.⁷² Its greatest disadvantage is that even minor alterations may easily remove the protection. Furthermore, if someone is aware that a document is protected in this manner, the watermark can be removed quickly and automatically.⁷³

To support the practical implementation of the transparency obligations under Articles 4 and 50 of the AI Act, the AI Office has initiated the development of a new Code of Conduct. The purpose of the Code is to provide detailed guidance on the appropriate labelling of AI-generated audio, image, video and textual content, thereby reducing the risks of manipulation, misinformation and identity misuse. The drafting process involves generative AI providers, developers of technical

⁷⁰ AI Act, Art. (2)-(4)

⁷¹ Fauchoux, V., *Transparency of AI-Generated Content: In-depth legal analysis of the Draft Code of Practice implementing Article 50 of the EU AI Act*, 2026, <https://www.ddg.fr/actualite/transparency-of-ai-generated-content-in-depth-legal-analysis-of-the-draft-code-of-practice-implementing-article-50-of-the-eu-ai-act>, 15 February, 2026.

⁷² Makhrib, Z. F.; Karim, A. A., *Digital Watermark Technique: A Review*, *Journal of Physics: Conference Series*, year 1999, 2021, p. 1.

⁷³ Pataki, M., *Algoritmusok egynyelvű és különböző nyelvek közötti fordítások és plágiumok megtalálására*,

PhD dissertation, Pázmány Péter Katolikus Egyetem, Információs Technológiai Kar, Multidiszciplináris Műszaki Tudományok Doktori Iskola, 2012. p. 14.

labelling solutions, civil society organisations, researchers and experts, and the final text is expected in May–June 2026.⁷⁴

Beyond Codes of Conduct, practical detection tools must target the distinctive features of deepfakes. These comprise biometric anomalies (unnatural blinking, irregular movements, unrealistic rendering), model-based fingerprints unique to the generating system, and media-based characteristics, including spatiotemporal inconsistencies and distortion noise. Analyzing these technical categories is essential for differentiating synthetic from authentic recordings.⁷⁵ Human observation is often insufficient to identify such discrepancies, whereas detection technologies and forensic methods increase the likelihood of accurate identification. In recent years, several software tools and online platforms have emerged, such as DeepFake-o-meter or FakeBuster, which are capable of detecting audiovisual manipulation. These platforms, however, remain in an early stage of development and require further refinement to keep pace with continuously evolving deepfake techniques.⁷⁶

State-of-the-art deepfake detection methods rely on deep learning to extract unique features. The most well-known architectures include Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) and their advanced variants. Examples are Long Short-Term Memory networks (LSTMs), a specialised type of RNN, and Residual Networks (ResNets), a more advanced form of CNN.⁷⁷ Also significant are hybrid approaches, such as combinations of CNN and RNN architectures, which may enhance detection accuracy. In such a system, the CNN extracts visual features from video frames, while the RNN analyses temporal relationships between frames to identify inconsistencies. This construction can, for instance, detect the absence of blinking. Its limitation is that it is effective only with short video clips—typically those lasting no more than two seconds—and relies solely on blink absence as an indicator. As a result, it is incapable of detecting manipulated recordings in videos with frequent blinking.⁷⁸⁷⁹

⁷⁴ European Commission, *Code of Practice on marking and labelling of AI-generated content*, <https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content>, 9 January, 2026.

⁷⁵ Zhang, T., *Deepfake generation and detection, a survey*, Multimedia Tools and Applications, 81/2022, p. 6264–6267.

⁷⁶ Masood, M.; Nawaz, M.; Malik, K. M.; Javed, A.; Irtaza, A.; Malik, H., *Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward*, *Applied Intelligence*, 1/2022, p. 25.

⁷⁷ Zhang, *op. cit.*, note 81, p. 6261–6264.

⁷⁸ Masood et al., *op. cit.*, note 82, p. 13.

⁷⁹ Zhang, *op. cit.*, note 81, p. 6261.

Despite many existing methods and combinations, each has limitations that affect its effectiveness depending on the content analysed.

5. FUTURE DIRECTIONS OF EU DIGITAL CHILD PROTECTION REGULATION

5. 1. Recast Directive

The European Union's child-protection framework is grounded in the Charter of Fundamental Rights, which in Article 24 enshrines the rights of the child to well-being and protection, as well as the principle that the child's best interests must be a primary consideration.⁸⁰ This legal foundation underpins Directive 2011/93/EU. The Directive sets out minimum EU rules concerning the definition of offences, sanctions, prevention and victim protection.⁸¹ Its recitals emphasise the severely rights-violating nature of child sexual abuse material,⁸² as well as the explosive growth of such material driven by the internet and emerging technologies, which justifies strengthened EU-level action.⁸³

Article 5 clearly defines the behaviours related to child sexual abuse material that Member States must criminalise, including acquisition or possession of CSAM, intentional access to such material, distribution, transmission or sharing, offering or making it available, and its production. These offences are punished at varying levels of severity, typically with imprisonment ranging from one to three years.⁸⁴

EU child-protection criminal law is now undergoing substantial reform, as the European Union seeks a regulatory framework better suited to addressing challenges of the digital age, particularly deepfakes and AI-generated content. The Recast Directive significantly revises and expands the conceptual and criminal-law framework applicable to child sexual abuse material—referred to in the updated terminology as "material depicting the sexual abuse of children." The Recast Directive introduces broader and clearer definitions, expressly encompassing content depicting persons appearing to be children; realistic digital images, including modified or entirely computer-generated material; reproductions and depictions of children such as avatars or other virtual characters;

⁸⁰ EU Charter Article 24

⁸¹ Klimek, L., *European responses criminalising online solicitation of children for sexual purposes*, Balkan Social Science Review, 6/2020, p. 13-14.

⁸² Directive 2011/93/EU, Preamble (1).

⁸³ Directive 2011/93/EU, Preamble (3).

⁸⁴ Directive 2011/93/EU, Article 5

and all non-visual formats providing guidance or instructions for the sexual abuse, exploitation or solicitation of children. The expanded definition aims to ensure that the legal framework covers deepfakes, AI-generated images and other technologically produced forms of abusive content. The Recast Directive clarifies that "realistic representation" includes any reproduction or digital rendering depicting children in a sexual context, and extends its scope to all material providing advice, guidance or instruction facilitating child sexual abuse, exploitation or solicitation. This would eliminate interpretative uncertainties present in the current Directive. Article 8(3) of the current Directive allows Member States to exempt certain content from criminal liability, provided it is created and possessed solely for private use, produced with mutual consent, and involves individuals above the national age of consent, without coercion or harassment. In practice, however, some Member States interpreted this exemption too broadly, applying it even in cases involving significant age or power imbalances while classifying such relationships as "peer situations." The Recast Directive therefore expands the scope of punishable conduct beyond the production and possession of material to include access, while also introducing stricter safeguards. The exemption is moved to Article 10 and applies only where the individuals concerned are above the age of consent and are genuine peers. The concept of a "genuine peer" is defined in Article 2 as persons "close in age and in psychological and physical maturity." Although the Recast Directive substantially broadens the concept of CSAM, debate continues over the extent to which purely virtual material—created without any real child—should be criminalised. The central issue concerns the legal basis for criminalisation and the potential harm caused by such content. Since these materials do not depict a real child, there appears to be no direct, identifiable victim at first glance.⁸⁵

However, this does not mean that such content is harmless. Research and regulatory developments clearly indicate that entirely virtual CSAM can normalise sexual abuse of children, encourage consumption of such material and contribute to its wider dissemination.⁸⁶ Deepfake-based material can negatively affect both depicted proxies and viewers, and therefore society as a whole.⁸⁷ Research indicates that AI-generated CSAM and similar phenomena can impose severe psychological burdens on affected individuals, increasing the risk of depression, anxiety, and even suicidal ideation. In addition, the consumption of virtual pornographic content can distort users' sexual attitudes and reinforce unrealistic

⁸⁵ Rigotti et al., *op. cit.*, note 27, p. 17-10.

⁸⁶ Dushi, *op. cit.*, note 14, p. 1.

⁸⁷ Karasavva, V.; Noorbhai, A., *The Real Threat of Deepfake Pornography: A Review of Canadian Policy*, Cyberpsychology, Behavior, and Social Networking, year 24, 3/2021, p. 207.

or harmful behavioural patterns, effects that deepfake technology further aggravates by enabling the creation of sexualised depictions of any person.⁸⁸

Virtual CSAM may also serve as a tool in the grooming process,⁸⁹ facilitating manipulation and trust-building while presenting lower detection risks compared with real CSAM. From a rational-choice perspective, offenders often turn to virtual CSAM because they perceive its benefits (sexual gratification, facilitation of contact, support for grooming) as outweighing the risks. Consumption of virtual material may therefore act as a gateway to offences against real children.⁹⁰

These concerns are reinforced by research showing that 52% of individuals who self-identify as offenders fear that their consumption of pornographic material could lead them to commit an actual offence. Thus, the absence of a real victim does not eliminate the societal risk; on the contrary, digital material may even constitute a first step towards real-world abuse.⁹¹

5.2. CSAR

In addition to the planned reforms of the criminal-law framework for child protection, the EU is also preparing a broader regulatory measure that would directly affect the operation of digital service providers. The proposed EU Regulation laying down rules to prevent and combat child sexual abuse (CSAR) represents a legislative effort to strengthen online child protection. The Commission presented the proposal on 11 May 2022, building on the 2020 EU Strategy, with the aim of establishing a harmonised response to the dissemination of child sexual abuse material and the online solicitation of children. The proposal seeks to impose mandatory risk-assessment, detection and reporting obligations on online service providers, including hosting services and end-to-end encrypted messaging applications such as WhatsApp and Signal.⁹²

⁸⁸ *Ibid.*, p. 204.

⁸⁹ Parti, *op. cit.*, note 49, p. 11-12.

⁹⁰ Christensen, L.; Moritz, D.; Pearson, A., *Psychological Perspectives of Virtual Child Sexual Abuse Material*, Sexuality & Culture, year 25, 4/2021, p. 1362.

⁹¹ Harkavy, R., EU moves to criminalise AI-generated CSAM, Global Legal Insights, 2025, <https://www.globallegalinsights.com/news/eu-moves-to-criminalise-ai-generated-csam/>, 12 February, 2026.

⁹² ASSEDEL (European Association for the Defense of Rights and Freedoms), *Regulation to Prevent and Combat Child Sexual Abuse (CSAR), policy analysis*, 2026, p. 1, https://assedel.org/wp-content/uploads/2026/01/1FINAL_Final-version-data-privacy-s.pdf, 17 February, 2026.

The emergence of EU-level rules aimed at combating online child sexual abuse developed in several stages. The first step was the adoption of the EU Interim Regulation 2021/1232, which temporarily allowed number-independent interpersonal communications services—such as webmail providers and messaging applications—to derogate voluntarily from the confidentiality and data-protection obligations set out in the ePrivacy Directive (2002/58/EC).⁹³ The aim was to permit providers to detect, report and remove CSAM.⁹⁴ The Interim Regulation was originally set to expire on 3 August 2024, but due to delays in adopting permanent legislation, its validity was extended to 3 April 2026. This extension places significant pressure on the EU legislature, as the expiry of the derogation would eliminate the existing legal framework for CSAM-screening practices.⁹⁵

In response, on 11 May 2022 the Commission presented a comprehensive, binding Regulation intended to replace the Interim Regulation. The Commission emphasised that the existing voluntary content-screening practices are fragmented, inconsistent in quality and generate legal uncertainty.⁹⁶ The proposed Regulation therefore aimed to replace the voluntary system with a uniform, mandatory mechanism for service providers, including risk-assessment and risk-mitigation requirements, CSAM detection, reporting obligations, removal of illegal material⁹⁷ and the prevention of online grooming.⁹⁸ The Commission also

⁹³ Rojszczak, M., *Preventing the dissemination of child sexual abuse material (CSAM) with surveillance technologies: The case of EU Regulation 2021/1232*, Computer Law & Security Review, year 56, 2025, p. 2-5.

⁹⁴ European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combating child sexual abuse online*, COM(2020) 568 final, Brussels, 2020, p. 1.

⁹⁵ European Parliament, *Legislative Train 12.2025 – New legislation to fight child sexual abuse online*, Legislative Train briefing, 2025, p. 2, <https://www.europarl.europa.eu/legislative-train/carriage/combating-child-sexual-abuse-online/report?sid=9801>, 12 January, 2026.

⁹⁶ European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*, COM(2022) 209 final, Brussels, 2022.

⁹⁷ ASSEDEL (European Association for the Defense of Rights and Freedoms), *Balancing Protection and Privacy in EU*, online commentary, 2026, <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February, 2026.

⁹⁸ Eurochild, *Eurochild reacts to the Council's position on the Regulation to Prevent and Combat Child Sexual Abuse*, news article, 2025, <https://eurochild.org/news/eurochild-reacts-to-the-councils-position-on-the-regulation-to-prevent-and-combat-child-sexual-abuse/>, 10 February, 2026.

proposed establishing a new independent EU Centre on Child Sexual Abuse (EUCSA) to support both service providers and authorities.⁹⁹

The proposal was reviewed by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), which began assessing it in 2022 and raised several concerns.¹⁰⁰ Supplementary impact assessments found that the proposal did not adequately address challenges inherent in end-to-end encrypted (E2EE) services. While detection of known CSAM is technically feasible, the identification of new material or grooming attempts remains uncertain. Interference with E2EE communication raises serious risks to the fundamental rights protected by Articles 7 and 8 of the Charter of Fundamental Rights—namely, the rights to privacy and data protection.¹⁰¹

The Commission's original proposal would have allowed authorities to require client-side scanning, obliging service providers to examine private messages. This generated extensive professional and civil opposition.¹⁰² The LIBE committee's draft report of 19 April 2023 supported the overall aims of the CSAR but proposed more than 1,900 amendments. These included extending the scope of the Regulation to search engines and other AI-based systems, and limiting CSA detection in E2EE services to metadata analysis only. The report also proposed establishing a victim consultation forum within the EUCSA and allowing voluntary detection practices to continue alongside mandatory measures.¹⁰³

⁹⁹ European Parliament, *Legislative Train 12.2025 – New legislation to fight child sexual abuse online*, *Legislative Train briefing*, 2025, p. 1, <https://www.europarl.europa.eu/legislative-train/carriage/combating-child-sexual-abuse-online/report?sid=9801>, 12 January, 2026.

¹⁰⁰ European Parliament, *Combating child sexual abuse online*, Briefing – EU Legislation in Progress, European Parliamentary Research Service (EPRS), 2025. p. 10, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI\(2022\)738224_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf), 29 January, 2026.

¹⁰¹ European Parliament, *Proposal for a regulation laying down rules to prevent and combat child sexual abuse – Complementary impact assessment*, European Parliamentary Research Service (EPRS), Brussels, 2023, p. 3, [https://www.ecorys.com/app/uploads/files/2023-05/EPRS_STU\(2023\)740248_EN.pdf](https://www.ecorys.com/app/uploads/files/2023-05/EPRS_STU(2023)740248_EN.pdf), 2 March 2025.

¹⁰² ASSEDEL (European Association for the Defense of Rights and Freedoms), *Balancing Protection and Privacy in EU*, *online commentary*, 2026, <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February, 2026.

¹⁰³ European Parliament, *Combating child sexual abuse online*, Briefing – EU Legislation in Progress, European Parliamentary Research Service (EPRS), 2025. p. 10, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI\(2022\)738224_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf), 29 January, 2026.

The Council's general approach, adopted on 26 November 2025, further diluted the Commission's original proposal. The Council rejected mandatory detection obligations but made the derogation from the ePrivacy Directive permanent. It introduced mandatory service-provider risk assessments and three risk categories (low, medium and high). High-risk services would be required to implement "risk-mitigation measures," of which scanning would be merely one possible option. Service providers that voluntarily participate in scanning could receive legal certainty and financial or classification advantages.¹⁰⁴ Under the new rules, providers must conduct risk assessments to prevent CSAM and grooming. National authorities oversee this process, holding the power to enforce corrective measures and mandate the removal of illegal content.¹⁰⁵ Trilogue negotiations began at the end of 2025, but adoption of the final text remains uncertain. Since the Interim Regulation will expire again in April 2026, the Commission considers an extension until 2028 necessary; otherwise, current CSAM-screening practices would lack a legal basis.¹⁰⁶

In essence, the legislative debate centres on how to balance effective measures against CSAM with full respect for privacy and data-protection rights, as proposals such as encrypted-communication scanning, detection algorithms, mandatory age verification and limits on anonymity risk becoming disproportionate and normalising digital surveillance.¹⁰⁷

6. CONCLUSIONS

The purpose of this study was to examine the gravity of the phenomenon of deepfake child sexual abuse material and to analyse how the European Union's existing and emerging legal frameworks respond to it. Statistical data clearly demonstrate that the volume of AI-generated synthetic sexualised depictions of children has increased at an exceptionally rapid pace in recent years and has now

¹⁰⁴ ASSEDEL (European Association for the Defense of Rights and Freedoms), *Balancing Protection and Privacy in EU, online commentary*, 2026, <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February, 2026.

¹⁰⁵ Eurochild, *Eurochild reacts to the Council's position on the Regulation to Prevent and Combat Child Sexual Abuse*, 2025, <https://eurochild.org/news/eurochild-reacts-to-the-councils-position-on-the-regulation-to-prevent-and-combat-child-sexual-abuse/>, 10 February, 2026.

¹⁰⁶ Moreau, C., *Commission proposes two-year extension to CSAM chat-scanning rules*, Euractiv, <https://www.euractiv.com/news/commission-proposes-two-year-extension-to-csam-chat-scanning-rules/>, 7 January, 2026.

¹⁰⁷ ASSEDEL (European Association for the Defense of Rights and Freedoms), *Balancing Protection and Privacy in EU, online commentary*, 2026, <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February, 2026.

become a particularly dangerous category of criminal activity. This dynamic growth presents new challenges for regulation, given that such material can be produced on a mass scale without necessarily involving real victims, yet remains capable of severely infringing the sexual integrity of children.

The analysis of EU law has shown that the European Union has recognised the specific characteristics of the phenomenon and is attempting to respond to the spread of AI-generated CSAM on multiple levels. With regard to the Recast Directive, the clarification of conceptual boundaries is of primary importance, as the proposal makes clear that both fully synthetic material and deepfake content incorporating the facial features or body parts of real children fall within the Union's definition of child sexual abuse material. The arguments presented demonstrate that although such material may lack an identifiable individual victim, it nevertheless violates the abstract legal interests associated with the sexual integrity and autonomy of children, thereby justifying an EU-level prohibition. Through the Recast Directive, the Union makes explicit that the object of protection is not limited to the bodily integrity of a specific child but extends more broadly to the collective legal interest in safeguarding children's sexual self-determination and development.

At the same time, the study has identified several unresolved issues, particularly in relation to the CSAR. The examination of encrypted communications raises significant fundamental-rights tensions, as it directly affects the rights guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights. Although the protection of children is a paramount EU objective, this does not exempt the legislator from the strict application of the principles of necessity and proportionality.

The analysis also highlights the limited effectiveness of the relevant provisions of the DSA and the AI Act. While both regulations contain rules that may touch upon aspects of AI-generated CSAM, neither provides a direct or comprehensive response to the phenomenon.

A de lege ferenda conclusion emerging from this study is that combating deepfake child sexual abuse material cannot be reduced merely to the introduction of new prohibitions or the expansion of criminal offences. Effective, sustainable and fundamental-rights-compliant regulation requires the coordinated application of criminal-law instruments, platform-governance mechanisms and artificial-intelligence regulation. Such an approach can only succeed if legal responses are developed in dialogue with technology developers, platform providers and civil-society actors. The future direction of EU regulation can be considered coherent and sustainable only if it ensures enhanced protection of

children while preserving the fundamental-rights balance inherent in the EU legal order.

REFERENCES

BOOKS AND ARTICLES

1. Boştăn, I., Consolidating the Role of AI in the Economy and Society: Combatting the Deepfake Phenomenon Through Strategic and Normative Approaches – The Case of Romania in the EU Context, *Economies*, year 13, 5/2025, p. 1–24.
2. Buri, I.; van Hoboken, J., The Digital Services Act (DSA) proposal: a critical overview, Discussion paper, Digital Services Act (DSA) Observatory, Institute for Information Law (IViR), University of Amsterdam, 2021, p. 1-43.
3. Burke, D. D.; Doval, C. N., Redefining child pornography in an age of technological advancement: The concept of avoidable harm, *Washington Journal of Law, Technology & Arts*, year 20, 3/2025, p. 44-66.
4. Charisi, V.; Chaudron, S.; Di Gioia, R.; Vuorikari, R.; Escobar Planas, M.; Sanchez, I.; Gomez, E., Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, 2022, p. 1-87
5. Christensen, L.; Moritz, D.; Pearson, A., Psychological Perspectives of Virtual Child Sexual Abuse Material, *Sexuality & Culture*, year 25, 4/2021, p. 1353–1365.
6. Ducret, M.; Wahal, E.; Gruson, D.; Amrani, S.; Richert, R.; Mouncif Mougache, M.; Schwendicke, F., Trustworthy Artificial Intelligence in Dentistry: Learnings from the EU AI Act, *Journal of Dental Research*, year 103, 11/2024, p. 1–6.
7. Dushi, D.; Berdufi, N.; Karagianni, A., The legal framework and legal gaps for AI generated child sexual abuse material, *Computer Law & Security Review*, 59/2025, Article Number 106094.
8. Furizal; Ma'arif, A.; Maghfiroh, H.; Suwarno, I.; Prayogi, D.; Kariyamin; Lonang, S.; Sharkawy, A.-N., Social, legal, and ethical implications of AI generated deepfake pornography on digital platforms: A systematic literature review, *Social Sciences & Humanities Open*, Year 12, 2025, p. 1-25.
9. Ganesh, H. K., Protecting Children Through Deepfake Child Pornography: A Moral, Legal, and Philosophical Discussion on the Intersection of the

- Evolution in Law and Technology, *American Criminal Law Review*, 60/2022, p. 1-15.
10. Genç Geleç, B., Regulating digital platforms: Will the DSA correct its predecessor's deficiencies?, *Croatian Yearbook of European Law and Policy*, year 18, 2022, p. 25–60.
 11. Gsell, Florence, The Digital Services Act (DSA): A General Assessment, In: von Ungern Sternberg, Antje (ed.), *Content Regulation in the European Union – The Digital Services Act*, TRIER Studies on Digital Law, year 1, Verein für Recht und Digitalisierung e.V., Institute for Digital Law (IRDT), Trier, 2023, p. 11-332
 12. Karasavva, V.; Noorbhai, A., The Real Threat of Deepfake Pornography: A Review of Canadian Policy, *Cyberpsychology, Behavior, and Social Networking*, year 24, p. 203–209.
 13. Kietzmann, J.; Lee, L. W.; McCarthy, I. P.; Kietzmann, T. C., Deepfakes: Trick or Treat?, *Business Horizons*, year 63, 2/2019, p. 135–146.
 14. Kim, B.-J.; Jeong, S.; Cho, B.-K.; Chung, J.-B., AI Governance in the Context of the EU AI Act, *IEEE Access*, 2025, p. 144126-144142.
 15. Klimek, L., European responses criminalising online solicitation of children for sexual purposes, *Balkan Social Science Review*, 6/2020, p. 7–21.
 16. Lendvai, G. F., Deepfake a szólásszabadság tükrében – reflexiók a jog perspektívájából, *Gondolat Kiadó*, Budapest, 2023, ISBN 978-963-556-465-1.
 17. Luan, T., A Survey on Deepfake Detection Technologies, *International Journal of Emerging Technologies and Advanced Applications*, 2/2025, p. 1-9.
 18. Makhrib, Z. F.; Karim, A. A., Digital Watermark Technique: A Review, *Journal of Physics: Conference Series*, year 1999, 2021, p. 1-10.
 19. Masood, M.; Nawaz, M.; Malik, K. M.; Javed, A.; Irtaza, A.; Malik, H., Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward, *Applied Intelligence*, 1/2022, p. 3974–4026.
 20. Negredo, L.; Herrero, Ó., Child pornography on the Internet, *Papeles del Psicólogo / Psychologist Papers*, year 37, 3/2016, p. 217-223.
 21. Novelli, C.; Casolari, F.; Rotolo, A.; Taddeo, M.; Floridi, L., Taking AI risks seriously: a new assessment model for the AI Act, *AI & Society*, year 39, 2024, p. 2493–2497.
 22. Parti, K.; Szabó, J.; The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe, *Laws*, year 13, 6/2024; Laws 78.
 23. da vidimPataki, M., Algoritmusok egynyelvű és különböző nyelvek közötti fordítások és plágiumok megtalálására, PhD dissertation, Pázmány Péter

- Katolikus Egyetem, Információs Technológiai Kar, Multidiszciplináris Műszaki Tudományok Doktori Iskola, 2012.
24. Patel, Y.; Tanwar, S.; Gupta, R.; Bhattacharya, P.; Davidson, I. E.; Nyameko, R.; Aluvala, S.; Vimal, V., Deepfake Generation and Detection: Case Study and Challenges, *IEEE Access*, 11/2023, p. 143296–143323.
 25. Rigotti, C.; Gkioka, C. P.; Do Rosario Da Graça, S.; Lannier, S., Overlapping offences, divergent logics: Reconciling EU law on sexual imagery of minors, *New Journal of European Criminal Law*, 2025, p. 3-26.
 26. Rojszczak, M., Preventing the dissemination of child sexual abuse material (CSAM) with surveillance technologies: The case of EU Regulation 2021/1232, *Computer Law & Security Review*, year 56, 2025. p. 1-14.
 27. Sandoval, M. P.; de Almeida Vau, M.; Solaas, J.; Rodrigues, L., Threat of deepfakes to the criminal justice system: a systematic review, *Crime Science*, year 13, 1/2024, p. 1-16.
 28. Schuett, J., Risk Management in the Artificial Intelligence Act, *European Journal of Risk Regulation*, year 15, 2/2023, p. 367–385.
 29. Sorbán, K., A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről, *Belügyi Szemle*, 10/2020, p. 81–104.
 30. Temir, E., Deepfake: New Era in The Age of Disinformation & End of Reliable Journalism, *Selçuk İletişim Dergisi*, 2/2020, p. 1009–1024.
 31. Veszelszki, Á., Deepfake: kételkedés a kételyben, In: Aczél, P.; Veszelszki, Á. (eds.), *Deepfake: a valótlan valóság*, Gondolat Kiadó, Budapest, 2023, p. 13–31.
 32. Weikmann, T.; Greber, H.; Nikolaou, A., After Deception: How Falling for a Deepfake Affects the Way We See, Hear, and Experience Media, *The International Journal of Press/Politics*, 1/2025, p. 187–210.
 33. Whittaker, L.; Mulcahy, R.; Letheren, K.; Kietzmann, J.; Russell, R.; Bennett, B., Mapping the deepfake landscape for innovation: A multidisciplinary systematic review and future research agenda, *Technovation*, 1/2023, p. 1–17.
 34. Wilman, Folkert, The Digital Services Act (DSA) – An Overview, working paper, European Commission, 2022, p. 1-21.
 35. Zhang, T., Deepfake generation and detection, a survey, *Multimedia Tools and Applications*, 81/2022, p. 6259–6276.
 36. Zverev, V.; Bushkov, V.; Khrushkov, B.; Sarychev, V.; Ostaltsev, O.; Prokopovych-Tkachenko, Y., Artificial intelligence and cybercrime: New challenges and prospects for legal regulation, *Contemporary Issues in Artificial Intelligence*, 1/2025, p. 1-8.

LEGAL RULES

1. Charter of Fundamental Rights of the European Union, Official Journal of the European Union, C 326, 26.10.2012.
2. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, OJ L 335, 17.12.2011.
3. European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, Brussels, 2022.
4. European Commission, Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number independent interpersonal communications service providers for the processing of personal and other data for the purpose of combating child sexual abuse online, COM(2020) 568 final, Brussels, 2020.
5. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC.
42. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), Official Journal of the European Union, L 2024/1689, 12.7.2024.

NETWORK RESOURCES

1. ASSEDEL (European Association for the Defense of Rights and Freedoms), Balancing Protection and Privacy in EU, online commentary, 2026, <https://assedel.org/regulation-to-prevent-and-combat-child-sexual-abuse-csar/>, 10 February, 2026.
2. ASSEDEL (European Association for the Defense of Rights and Freedoms), Regulation to Prevent and Combat Child Sexual Abuse (CSAR), policy analysis, 2026, https://assedel.org/wp-content/uploads/2026/01/1FINAL_Final-version-data-privacy-s.pdf, 17 February, 2026.

3. Choudhary, A. S., What is Variational Autoencoders? Data Science Blogathon 2025, <https://www.analyticsvidhya.com/blog/2023/07/an-overview-of-variational-autoencoders/>, 22 April, 2025.
4. Elcano Royal Institute, Risk without borders: the malicious use of AI and the EU AI Act's global reach, Analysis, <https://www.realinstitutoelcano.org/en/analyses/risk-without-borders-the-malicious-use-of-ai-and-the-eu-ai-acts-global-reach/>, 10 February, 2026.
5. Eurochild, Eurochild reacts to the Council's position on the Regulation to Prevent and Combat Child Sexual Abuse, news article, 2025, <https://eurochild.org/news/eurochild-reacts-to-the-councils-position-on-the-regulation-to-prevent-and-combat-child-sexual-abuse/>, 10 February, 2026.
6. European Commission, AI Act, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>, 14 November, 2025.
7. European Commission, Code of Practice on marking and labelling of AI generated conten, <https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content>, 9 January, 2026.
8. European Commission, Digital Services Act: keeping us safe online, 2025, https://commission.europa.eu/news-and-media/news/digital-services-act-keeping-us-safe-online-2025-09-22_en, 19 December, 2025.
9. European Commission, Supervision of the designated very large online platforms and search engines under the Digital Services Act, <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>, 10 February, 2026.
10. European Commission, The Digital Services Act, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>, 8 October, 2025.
11. European Commission, The enforcement framework under the Digital Services Act, <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement>, 19 February, 2026.
12. European Data Protection Board (EDPB), Guidelines 3/2025 on the interplay between the Digital Services Act and the GDPR, 2025, https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202503_interplay-dsa-gdpr_v1_en.pdf, 10 December, 2025.
13. European Newsroom (ENR), Nudification blocks: The EU's struggle for more safety online, News article, 2026, <https://europeannewsroom.com/nudification-blocks-the-eus-struggle-for-more-safety-online/>, 6 February, 2026.
14. European Parliament, Combating child sexual abuse online, Briefing – EU Legislation in Progress, European Parliamentary Research Service (EPRS), 2025,

- [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI\(2022\)738224_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf), 29 January, 2026.
15. European Parliament, Legislative Train 12.2025 – New legislation to fight child sexual abuse online, Legislative Train briefing, 2025, <https://www.europarl.europa.eu/legislative-train/carriage/combating-child-sexual-abuse-online/report?sid=9801>, 12 January, 2026.
 16. European Parliament, Proposal for a regulation laying down rules to prevent and combat child sexual abuse – Complementary impact assessment, European Parliamentary Research Service (EPRS), Brussels, 2023, [https://www.ecorys.com/app/uploads/files/2023-05/EPRS_STU\(2023\)740248_EN.pdf](https://www.ecorys.com/app/uploads/files/2023-05/EPRS_STU(2023)740248_EN.pdf), 2 March 2025.
 17. European Parliament, Children and deepfakes, Briefing, European Parliamentary Research Service (EPRS), 2025, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf), 12 February, 2026.
 18. Fauchoux, V., Transparency of AI Generated Content: In depth legal analysis of the Draft Code of Practice implementing Article 50 of the EU AI Act, 2026, <https://www.ddg.fr/actualite/transparency-of-ai-generated-content-in-depth-legal-analysis-of-the-draft-code-of-practice-implementing-article-50-of-the-eu-ai-act>, 15 February, 2026.
 19. Harkavy, R., EU moves to criminalise AI generated CSAM, Global Legal Insights, 2025, <https://www.globallegalinsights.com/news/eu-moves-to-criminalise-ai-generated-csam/>, 12 February, 2026.
 20. Internet Watch Foundation (IWF), How AI is being abused to create child sexual abuse imagery, institutional report, 2023, https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf, 18 January, 2026.
 21. Internet Watch Foundation (IWF), What has changed in the AI CSAM landscape?, AI CSAM Report Update, Version 1.1, July 2024, https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf, 5 January, 2026.
 22. Introduction to diffusion models for machine learning. Superannotate 2025, <https://www.superannotate.com/blog/diffusion-models#:~:text=Diffusion%20models%20are%20prominent%20in,distribution%20from%20the%20noisy%20data>, 25 June, 2025.
 23. Moreau, C., Commission proposes two-year extension to CSAM chat-scanning rules, Euractiv, <https://www.euractiv.com/news/commission-proposes-two-year-extension-to-csam-chat-scanning-rules/>, 7 January, 2026.
 24. O'Connor, R., Introduction to Diffusion Models for Machine Learning, Assemblyai 2022, <https://www.assemblyai.com/blog/diffusion-models-for-machine-learning>

introduction#:~:text=Let's%20dive%20in!,Diffusion%20Models%20%2D
%20Introduction,through%20the%20learned%20denoising%20process, 30
June, 2025.

25. Sensity, How to Detect a Deepfake Online: Image Forensics and Analysis of Deepfake Videos, 2021, <https://sensity.ai/blog/how-to-detect-a-deepfake/>, 24 June, 2025.
26. U.S. Department of Homeland Security – Homeland Security Investigations, Artificial Intelligence and Combating Online Child Sexual Exploitation and Abuse, Know2Protect campaign, online infographic, https://www.dhs.gov/sites/default/files/2024-09/24_0920_k2p_genai-bulletin.pdf, 3 January, 2026.

UDK: 347.4 : 004.75
347 : 004
Review paper

Józsa Ede, PhD student
Faculty of Law, University of Miskolc, Hungary
E-mail: jozsaede@gmail.com
ORCID ID: 0009-0006-8085-7910

RETHINKING THE CONCEPT OF CONTRACTUAL FREEDOM IN THE ERA OF SMART CONTRACTS

ABSTRACT

This study examines how the proliferation of smart contracts in the digital environment reshapes the classical legal principle of freedom of contract. The analysis proceeds from the three foundational pillars of contractual autonomy embedded in the continental private law tradition: the freedom to conclude a contract, the freedom to choose one's contracting partner, and the freedom to determine the content of the contract. Of these three dimensions, smart contracts meaningfully preserve only the first, while substantive autonomy is significantly constrained by pre-coded contractual terms. On the basis of the "code as law" approach, contractual legal relationships are governed by technical structures that exclude classical negotiation and flexibility between the parties. Employing a legal-theoretical methodology, the study analyses the implications of this transformation and concludes that, although freedom of contract formally persists, it requires substantive reinterpretation within the framework of technological determinism.

Keywords: *freedom of contract, smart contract, blockchain technology, digital private law, technological determinism.*

1. INTRODUCTION

Freedom of contract, as one of the fundamental principles of classical liberalism¹, is firmly embedded in continental private law² thinking. According to this tradition, contract formation is based on the free decision of autonomous legal

¹ According to classical liberalism, the source of law is not the will of the state, but the natural legal order derived from individual freedoms. Consequently, the purpose of law is not the enforcement of state will, but the protection of individual liberty even against the state. Szabó, G., *The Human Rights Risks of Globalisation*, PhD Dissertation, University of Pécs, Pécs 2008, pp. 157–158.

² Continental private law denotes a codified system of private law based on Roman legal traditions, characteristic primarily of continental European countries. This continental model stands in sharp contrast to the Anglo-Saxon common law system, where legal development is based on judicial decisions and precedents.

subjects: the parties may, at their own discretion, choose their contracting partners and determine the content of the contract.

With the advance of digitalisation and the spread of smart contracts³, however, the normative content of this principle requires reconsideration. The smart contract – a blockchain-based⁴ construction capable of automatic execution – is not merely a technical innovation, but also signals a profound structural transformation of contractual mechanisms.

The central question of this study is whether freedom of contract, as a classical legal principle, can prevail in the digital environment of smart contracts. The hypothesis of the analysis is that freedom of contract formally continues to exist, yet becomes substantively constrained. While the parties may decide whether to enter into a contract, the contractual terms – such as price or the mode of performance – are typically predetermined; consequently, actual autonomy is reduced to a choice among predefined options.

The methodology of the study is grounded in legal-theoretical analysis, juxtaposing the conceptual foundations of classical freedom of contract⁵ with the theoretical frameworks of digital determinism⁶, with particular attention to those views according to which code assumes a normative function equivalent to that of law.

The aim of the study is to demonstrate that, with the proliferation of smart contracts, freedom of contract does not disappear, but its function and meaning are transformed: it can no longer be interpreted as classical autonomy, but is instead reduced to a technologically framed freedom of choice.

³ For the purposes of the present research, the concept of a smart contract is defined as code containing if-then logical instructions that executes itself automatically when the previously specified condition(s) are fulfilled.

⁴ Blockchain is a distributed data structure that records events occurring on a network in the form of a chain of timestamped data blocks.

⁵ Classical freedom of contract is based on the principle of maximum autonomy, according to which contracting parties are free to decide whether to conclude a contract, with whom, and with what content. State intervention is justified only in exceptional and well-founded cases. See further: Szalai, Á., *The Content of the Contract*, Pázmány Law Working Papers, 2013/11.

⁶ Digital determinism is a social-scientific and philosophical theory according to which the development of digital technology determines the structure, functioning, and future of society. According to this view, technology is not merely a tool, but an autonomous, decisive force shaping economic, political, and cultural processes.

2. THE CLASSICAL THEORETICAL FOUNDATIONS OF FREEDOM OF CONTRACT

The first issue to be examined with regard to the formation of a contract is the existence of contractual intent, the absence of which entails the sanction of invalidity. In the context of smart contracts, the process through which contractual intent is formed differs markedly from the classical manifestation of intent known from traditional contract formation, which typically appears in written form, often embodied in a signature. In the case of smart contracts, contract formation takes place on the basis of conditions embedded in computer code, usually determined by a third party. Consequently, in my view, the contractual intent of the parties is essentially directed towards the acceptance or rejection of the pre-programmed contractual terms.

Thus, the classical formation of a contract is based on the mutual agreement of the parties, which may, in certain cases, have to comply with specific formal requirements in order to be valid. By contrast, smart contracts are concluded on the basis of predetermined terms that the parties cannot modify – only accept or reject – so that personal negotiation and bargaining play no role.

It can generally be stated that the civil law provisions of most legal systems predominantly consist of dispositive rules. As an example, one may examine the principle of freedom of contract, which is recognised and guaranteed by both the Hungarian and Romanian legal systems⁷.

A consequence of the existence of freedom of contract as a fundamental principle of private law is that the contracts regulated within a given legal system do not constitute a closed list, since contracts, in terms of type and content, are limited only by the imagination of the parties, insofar as they do not conflict with statutory

⁷ Civil Code, Act V of 2013 (Hungary), Section 6:59 (Freedom of Contract):

"(1) The parties may freely conclude a contract and may freely choose the other contracting party. (2) The parties may freely determine the content of the contract. By concordant intention, they may deviate from the rules governing the rights and obligations of the parties, unless this Act prohibits such deviation."; Civil Code (Romania), Art. 1169: *"The parties may freely conclude any contract and determine its content, within the limits laid down by the law, public order, and public morals."* As regards the codified formulation of freedom of contract, Art. 1169 of the Romanian Civil Code captures the essence of the principle more succinctly and more precisely than Section 6:59 of the Hungarian Civil Code. While the Hungarian provision separates substantive and personal freedom, the Romanian rule presents them jointly within a single paragraph and additionally supplements them with limiting clauses of public order and public morals. The sanction of nullity for conflict with good morals is regulated as a separate provision in the Hungarian Civil Code, whereas the Romanian Civil Code addresses this in an integrated manner.

prohibitions or with the requirements of public order and public morals/good morals⁸.

The principle of freedom of contract is a cornerstone of civil law dogmatics, ensuring not only the autonomy of the parties but also constituting a foundational pillar of the legal structure of the market economy. Freedom of contract is based on consensus between individuals, brought about by their autonomous will; it is therefore also an expression of private autonomy. As demonstrated by both Hungarian and European legal development, this principle has manifested itself differently in various historical and economic contexts; nevertheless, the dogmatics of contract formation has consistently proceeded from this fundamental principle⁹.

Freedom of contract may also be understood as a fundamental-rights dimension of the market economy. According to classical private law thinking, this autonomy is grounded in agreement between the parties, which the state merely frames but does not shape. The development of Hungarian private law has likewise followed this logic: the contract is not merely a legal act, but a forum for the expression of individual free will¹⁰.

Freedom of contract is therefore a central principle of classical private law, closely linked to the philosophical and political foundations of bourgeois society. This principle acquired its normative weight during the emergence of modern codified private law, within the ideological framework of eighteenth- and nineteenth-century classical liberalism. The roots of this freedom can be traced to Enlightenment thinkers, in particular the theories of Locke¹¹ and Kant¹².

In Locke's conception of the state based on the social contract, emphasis is placed on the protection of individual self-determination and the right to property. From Kant's moral philosophy, contract formation may be derived as an expression of autonomous will: a contract is nothing other than the lawful union of two wills.

⁸ Civil Code, Act V of 2013 (Hungary), Section 6:59; Civil Code (Romania), Art. 1169.

⁹ Török, É., *Fundamental Issues of Contract Formation*, Debrecen 2013, pp. 14–29.

¹⁰ Török, É., *op. cit.*, pp. 14–29.

¹¹ John Locke (1632–1704): he is regarded as the father of English classical liberalism. Locke's political philosophy fundamentally determined the modern understanding of democracies and human rights. Locke emphasised the right to property and free action – these constitute the moral foundations of the private-law conception of freedom.

¹² Immanuel Kant (1724–1804): one of the greatest figures of modern ethical science and legal philosophy, and a central figure of German idealism. According to Kant, a contract is the coordination of legally mutually recognised wills – this is one form of the realisation of autonomy.

Within continental legal systems, the scholars of the Pandectist tradition¹³ – most notably Savigny¹⁴ – elevated freedom of contract to the level of dogmatics. According to Savigny, law is the legally regulated relationship of wills; consequently, the entire system of private law rests upon the principle of individual autonomy. Both the German Civil Code (BGB) and the French Code civil were founded on this philosophical basis, emphasising that the state merely provides the external framework for contract formation, while the determination of content depends on the autonomy of the parties.

Classical doctrine distinguishes three dimensions of freedom of contract: (1) freedom to conclude a contract (*voluntas contrahendi*); (2) freedom to choose one's contracting partner (*libertas eligendi*); and (3) freedom to determine the content of the contract (*libertas determinandi*)¹⁵.

This tripartite structure represented the full realisation of private autonomy in the classical sense. At the same time, this principle was never entirely unlimited. From the first half of the twentieth century onwards, the recognition of economic inequalities and social embeddedness made it necessary to reinterpret freedom of contract. The school of social private law¹⁶ (e.g. Rudolf von Jhering¹⁷, Otto von

¹³ The Pandectists were representatives of nineteenth-century German legal scholarship who, on the basis of the dogmatic processing of Roman law, sought to create a theoretically coherent and systematised structure of private law. Their name refers to the *Pandectae*, that is, the Digest of Justinian, which was the principal source collection of classical Roman law. Their aim was to construct, on these historical foundations, a modern legal system built on logical principles.

¹⁴ Friedrich Carl von Savigny (1779–1861): one of the most influential German jurists of the nineteenth century, the founder of the Historical School of Law (*Historische Rechtsschule*), who reformed European private-law scholarship. His critique of French-style codification opened fundamentally new paths in continental legal development. According to Savigny, law is not an "artificial" creation that can be produced in an instant (e.g. by codification), but an organic process of development rooted in the spirit of the people.

¹⁵ Some authors apply a fourfold division of freedom of contract: (1) freedom to conclude a contract; (2) freedom to choose a contracting partner; (3) freedom of type; and (4) freedom to determine content. Béky, Á. E., *The Interpretation of Freedom of Contract in Modern Civil Law*, Debrecen, available at: <https://dea.lib.unideb.hu/server/api/core/bitstreams/a7787bc4-a990-4863-a2a9-d70bad5a31b4/content>, 25 February 2026.

¹⁶ Social private law is a legal conception that supplements the classical private law's equality-based, formally neutral contractual and property relations with social responsibility and inequality correction. The central aim of this approach is that private law – in particular contract and property law – should ensure not only market freedom, but also the protection of the weaker party.

¹⁷ Rudolf von Jhering (1818–1892): the father of "purpose in law" (*Zweckrecht*), one of the most influential figures of German legal scholarship. At first he followed the theoretical

Gierke¹⁸⁾ pointed out that inequalities can in fact distort the free manifestation of will. This line of thought was further deepened in the second half of the twentieth century, particularly under the influence of realist and critical legal theories¹⁹⁾. We thus arrive at the following conclusion: the "formal neutrality" of law does not guarantee actual autonomy if the economic or technological environment determines contractual positions.

Classical freedom of contract was therefore historically linked to a specific social and economic model – industrial capitalism and the principle of national sovereignty. The expansion of digital technologies begins to blur the boundaries of this model, once again raising the question: under what conditions can we today speak of meaningful contractual autonomy? This question becomes especially salient in the world of smart contracts, where contractual terms are no longer the result of free negotiation between the parties, but rather pre-coded, algorithmic structures.

3. THE OPERATION AND CHARACTERISTICS OF SMART CONTRACTS

In the present chapter, concepts are introduced whose definition is of key importance for understanding the operational mechanism of smart contracts. First, the discussion will begin with an outline of the notions arising in connection with blockchain technology.

Second, the definitions of smart contracts employed in the scholarly literature will be examined, and their conceptual scope will be delineated by formulating an autonomous definition.

3.1. Concepts related to Blockchain Technology

traditions of the Pandectists, then later took a critical turn and emphasised the social purpose and function of law.

¹⁸⁾ Otto von Gierke (1841–1921): a forerunner of "social private law", the developer of the community theory of legal persons. Proceeding from the heritage of the German Historical School, Gierke radically rethought the relationship between law and community.

¹⁹⁾ In the second half of the twentieth century, several realist and critical trends appeared in legal theory that rejected formalist, objectivist, or idealist approaches to law, and instead emphasised social, political, economic, psychological, and moral contexts. Such movements include, for example: American Legal Realism, Scandinavian Realism, Critical Legal Studies, Feminist Legal Theory, and Critical Race Theory.

Blockchain is a distributed data structure that records events occurring on a network²⁰ in the form of a chain of timestamped data blocks²¹. It operates in a decentralised manner, meaning that the data are not maintained by a central authority; rather, the ledger²² is jointly maintained by the participating nodes²³ of the network through peer-to-peer connections²⁴. In addition to a list of transactions, each block contains the cryptographic hash value²⁵ of the previous block, thereby ensuring the retrospective immutability of the data chain.

Transactions carried out on a blockchain network are authenticated through asymmetric cryptography²⁶: each user possesses a public and a private (secret)

²⁰ Christidis, K.; Devetsikiotis, M., *Blockchains and Smart Contracts for the IoT*, Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC, USA 2016, p. 2293.

²¹ A block is the basic unit of a blockchain, containing a collection of validated transactions and the hash of the previous block, thereby ensuring the continuity and immutability of the chain within a decentralised, cryptographically protected system. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K., *Blockchain Technology Overview*, National Institute of Standards and Technology (NIST), 2018, DOI:10.6028/NIST.IR.8202.

²² A distributed ledger is a data structure whose purpose is to provide final, unambiguous, and immutable data storage, in such a way that the data are distributed across a network of computers (nodes). ISO 22739:2020 – *Blockchain and distributed ledger technologies — Vocabulary*; European Union Blockchain Observatory and Forum, *Legal and Regulatory Framework of Blockchains and Smart Contracts in the EU*, 2020.

²³ In the crypto world, nodes are devices that essentially enable the operation of the blockchain network. *What is a node?*, CoinCash, available at: <https://hu.coincash.eu/kripto-szotar/n/node>, 25 February 2026.

²⁴ The peer-to-peer (P2P) model in digital data exchange denotes a network structure in which the participating parties are directly connected to each other without a technical intermediary. This model enables users to conduct transactions without involving a financial institution. Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, p. 1; <https://bitcoin.org/bitcoin.pdf>, 25 February 2026.

²⁵ Cryptographic hashing is a one-way mathematical process that generates a fixed-length unique identifier (hash) from arbitrary data. The hash value guarantees data integrity: if any part of the data changes, the hash will be completely different. This property is particularly significant in contractual and evidentiary environments, where data immutability and traceability are fundamental requirements.

²⁶ Cryptography is a field encompassing the principles, tools, and methods used to transform data in order to conceal their semantic content, prevent unauthorised use, and exclude undetectable modification.

key²⁷, enabling the creation and verification of digital signatures. The nodes validate transactions on the basis of a predetermined consensus mechanism²⁸.

One of the best-known consensus mechanisms is Proof of Work (PoW²⁹), in which miners responsible for validating blocks "compete" by solving computational tasks; the winning node may create the new block and receives cryptocurrency as a reward. An alternative is Proof of Stake (PoS³⁰), which, instead of computational capacity, is based on the validator's stake or wealth.

Blockchain is not a single, uniform technology, but rather a configurable architecture adaptable to various purposes. Blockchains may be distinguished according to access: (1) public blockchains³¹ (e.g. Bitcoin, Ethereum), which are open to anyone wishing to participate; (2) private blockchains³², accessible only to designated participants; and (3) permissioned and permissionless systems, differentiated according to whether authorisation is required for participation or for conducting transactions.

²⁷ The security of blockchain networks is ensured by asymmetric cryptography, also known as public/private key cryptography, where each participant has a publicly accessible public key and a secret, exclusive private key. Using the public key, anyone may send a transaction or verify a digital signature, while the private key authorises the signing of transactions and the transfer of assets. Nakamoto, S., op. cit., p. 2; Mozilla Foundation, *How public key encryption works*, available at: <https://developer.mozilla.org/en-US/docs>, 25 February 2026.

²⁸ Nodes operating a blockchain must agree on which transactions are included and in what order they appear in the new block. In the absence of such agreement, different instances of the blockchain would evolve differently, leading to so-called forks; nodes would reflect different "world states", and the network would be unable to maintain a uniform, authentic chronology (i.e. a blockchain), unless the given fork is resolved. Greenspan, G., *Avoiding the Pointless Blockchain Project*, 2015, available at: <https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/>, 25 February 2026.

²⁹ Proof of work is a process in which miners (those who solve complex cryptographic tasks and thereby validate transactions and create new blocks on the blockchain) receive a reward from the algorithm. German, P., *What Is Proof of Stake and Proof of Work?*, CryptoFalka, available at: <https://cryptofalka.hu/proof-of-work-proof-of-stake/>, 25 February 2026.

³⁰ Proof of stake emerged as an alternative to proof of work, as it requires significantly less computational capacity for block creation. In PoS systems, a node's chance of creating the next block is proportional to the balance held by that node. Buterin, V., *On Stake*, 2014, available at: <https://blog.ethereum.org/2014/07/05/stake/>, 31 May 2025.

³¹ *What Are the 4 Different Types of Blockchain Technology?*, TechTarget, available at: <https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology>, 25 February 2026.

³² European Law Institute, *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection*, European Union's Justice Programme, 2022, p. 25., available at: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology_Smart_Contracts_and_Consumer_Protection.pdf, 25 February 2026.

A key feature of blockchain operation is the so-called trustless network. The execution of transactions between parties does not require an intermediary, as the functioning of the system is ensured by technical consensus among nodes rather than by an external authority. This distributed trust model may constitute one of the foundational pillars of the digital economy.

3.2. The concept of the Smart Contract

The concept of the smart contract was coined by the Hungarian computer scientist and engineer Nick Szabo. According to his definition, a smart contract is "*a transactional protocol that executes the terms of a contract*"³³.

In Szabo's vision, basic contractual forms can be embedded into computer software as well as hardware, and through these means contract formation can be automated. According to Szabo's proposal, contractual provisions – such as securities, undertakings, and similar arrangements – may be fixed through coding, and their embedding into hardware or software devices enables the autonomous enforcement of the agreement once the stipulated conditions are fulfilled³⁴. As a result, the need for trusted intermediaries may become unnecessary – the existence of trust between the contracting parties is replaced not by a third party, but by technology – and contractual disputes may be minimised.

According to Szabo's view, a typical example of smart contracts can be interpreted as a purchase from a vending machine, during which the system dispenses the product without human intervention. This approach, however, is debatable, since in this case it is not the contract itself that can be regarded as "smart", but rather the device that performs the obligation on behalf of the operator. Nevertheless, the example – although it does not fully reflect the substantive characteristics of smart contracts – illustratively demonstrates one effect of digitalisation, namely that a machine system performs contractual obligations in place of the legal subject.

³³ Csítei, B., *Smart Contracts*, Opuscula Civilia, 2019, p. 6, available at: https://antk.uni-nke.hu/document/akk-copy-uni-nke-hu/Opuscula_Civilia_2019_Csitei_Bela.pdf, 26 March 2025; Szabo, N., *Smart Contracts*, 1994, available at: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>, 25 February 2026.

³⁴ Szabo, N., *The Idea of Smart Contracts*, 1997, available at: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabs.best.vwh.net/idea.html>, 25 February 2026.

Particular attention should be paid to the definition provided by Ágnes Juhász, who describes the technology as follows: "*In the simplest and most concise formulation, a smart contract is nothing other than a self-executing agreement*"³⁵.

The definitions offered by the aforementioned authors highlight the importance of different attributes; however, a common element is the self-executing nature of the contract.

It is reasonable to examine and use as a point of departure the definition contained in the document issued by the European Union in September 2019 establishing the legal regulatory framework for blockchain and smart contracts, according to which a smart contract is "*computer code that is stored on a blockchain and accessible by one or more parties (...) and is often self-executing*"³⁶.

Taking these characteristics and definitions into account, within the framework of the present study the concept of a smart contract is defined as code containing if-then logical instructions that executes itself automatically when the previously specified condition(s) are fulfilled³⁷.

A smart contract is a script written onto a blockchain that is executed automatically, has a unique address, and is activated by sending a transaction. The execution of the contract takes place simultaneously and deterministically on every node of the network, which guarantees uniform network consensus. Architecturally, the system operates as a distributed virtual machine in which each node runs the same program on the basis of identical inputs.

The contract code is public and auditable, and interactions with it are recorded on the blockchain in the form of digitally signed messages, thereby ensuring full cryptographic traceability.

³⁵ Juhász, Á., *Online Contracting, Digital Content and Services, Smart Contracts – A New Era of Contract Law?*, Infocommunication and Law, 2020/2, (75.) e-special issue, available at: <https://infojog.hu/juhasz-agnes-online-szerzodeskotes-digitalis-tartalom-es-szolgaltatas-intelligens-szerzodesdel-a-szerzodesi-jog-uj-korszaka-2020-2-75-e-kulonszam/>, 25 February 2026.

³⁶ "*In the blockchain context, it generally means computer code that is stored on a blockchain and that can be accessed by one or more parties. These programs are often self-executing and make use of blockchain properties like tamper-resistance, decentralised processing, and the like.*" Lyons, T.; Courcelas, L.; Timsit, K., *Legal and Regulatory Framework of Blockchains and Smart Contracts – A Thematic Report Prepared by the European Union Blockchain Observatory and Forum*, 27 September 2019, p. 22.

³⁷ For example, an operation executed by a smart contract may be the following: if a certain amount is credited to a bank account, then 10% of that amount is transferred to a second bank account for long-term savings purposes.

3.3. The operational mechanism of Smart Contracts – a practical example

In the following, a practical example³⁸ is presented in order to illustrate the operational mechanism of a smart contract.

Let us consider a blockchain network in which Alice, Bob, and Carol participate, and in which digital assets of type X and Y are traded. Bob deploys a smart contract on the network containing the following functions: (a) a "deposit" function that allows him to place units of X into the contract; (b) a "trade" function that returns 1 unit of X (from the assets previously deposited into the contract) in exchange for every 5 units of Y; and (c) a "withdraw" function that allows Bob to retrieve the entire asset balance held by the contract.

In our example, the "deposit" and "withdraw" functions are written in such a way that only Bob (via his private key) can activate them. This is Bob's design choice made at the time of programming, and within the framework of this example it is reasonable; however, in theory, these functions could also be written so that any network user may activate them.

Next, Bob initiates a transaction to the smart contract's address, activates the "deposit" function, and transfers 3 units of X into the contract. This transaction is recorded on the blockchain. Subsequently, Alice – who possesses 12 units of Y – sends a transaction to the "trade" function, transferring 10 units of Y to the contract and, in return, receiving 2 units of X. This transaction is likewise recorded on the blockchain. Finally, Bob sends a signed transaction to the "withdraw" function: the contract verifies the signature in order to ensure that the withdrawal is indeed initiated by the owner of the contract. Thereafter, it transfers the entire asset balance held by the contract to Bob (1 unit of X and 10 units of Y).

The example clearly demonstrates that the parties' freedom of decision is heavily based on data-driven logic. Individual will does not appear in the classical sense (free negotiation, shaping of contractual content), but is limited to the activation of a pre-programmed behavioural system. Freedom of contract therefore formally persists – one may decide whether to interact with the contract – but substantively it is deterministically defined, meaning that the sphere of autonomous decision-making is narrowed.

³⁸ Christidis, K.; Devetsikiotis, M., *op. cit.*, p. 2296.

This confirms the central hypothesis of the study: classical freedom of contract operates in a diminished form in the environment of smart contracts, as machine code and condition-driven logic take the place of individual autonomy.

4. NEW CHALLENGES TO FREEDOM OF CONTRACT IN THE AGE OF SMART CONTRACTS

The transformation of freedom of contract in the context of smart contracts requires a twofold analysis: one which situates these mechanisms within the tradition of standardised contracting, and another that captures the qualitatively new constraints arising from their technological architecture.

4.1. Smart Contracts and Standard Form Contracts: Continuity or Rupture?

At this point, it is necessary to nuance the above thesis by situating smart contracts within the broader evolution of contractual practice. The limitation of contractual autonomy observed in smart contracts is not entirely without precedent in classical private law systems. In particular, standard form contracts and adhesion contracts have long represented situations in which one party's ability to negotiate contractual terms is significantly restricted³⁹.

In the case of standard terms, contractual content is typically pre-formulated by one party, while the other party is limited to a binary choice: acceptance or rejection⁴⁰. From this perspective, the reduction of autonomy to a "take-it-or-leave-it" decision is not a novel phenomenon introduced by digital technologies, but rather an already existing structural feature of modern mass contracting.

However, the structural logic underlying these two models differs in a fundamental respect. In classical adhesion contracts, the "take-it-or-leave-it" mechanism reflects an asymmetry between the parties: the stronger party unilaterally determines the contractual content, while the weaker party is left with no real

³⁹ Waraich, R. S.; Fayaz, M.; Zahid, H., *Consent Theory and Adhesion Contract: A Critical Analysis of Contemporary Global Business Practices*, 2022, p. 2., available at: https://www.researchgate.net/publication/365964837_Consent_Theory_and_Adhesion_Contract_A_Critical_Analysis_of_Contemporary_Global_Business_Practices, 25 February 2026.

⁴⁰ Ben-Shahar, O., *Boilerplate and the Foundations of Contract Law*, Cambridge University Press, 2007, p. 7., available at: https://assets.cambridge.org/97805216/76380/frontmatter/9780521676380_frontmatter.pdf, 25 February 2026.

possibility of influencing its terms⁴¹. The restriction of contractual autonomy is therefore not symmetrical, but is instead rooted in unequal bargaining power and economic dominance.

By contrast, in the environment of smart contracts, this asymmetry is, in principle, absent. Neither contracting party typically determines the contractual terms in the course of the contractual relationship; rather, both parties are equally subjected to a pre-existing coded structure. The "take-it-or-leave-it" logic thus applies to all participants in a uniform manner: each party must accept or reject the conditions embedded in the code, without the possibility of unilateral modification. In this sense, the limitation of contractual autonomy is no longer the consequence of a hierarchical relationship between the parties, but is instead inherent in the technological framework itself.

A further distinction may be observed with regard to the origin of contractual content. In the case of standard form contracts, the stronger party actively shapes the contract by drafting pre-formulated terms tailored to its own interests. In contrast, smart contracts are typically developed independently of the concrete contractual relationship, often by programmers or platform operators, and are subsequently used by parties who merely interact with the existing code. As a result, neither party exercises direct control over the content of the contract at the moment of contracting.

Admittedly, exceptional situations may arise in which one of the contracting parties also assumes the role of programmer and thereby determines the contractual logic. In such cases, a structural asymmetry comparable to that of adhesion contracts may reappear. Nevertheless, this should be regarded as a special configuration rather than the general model of smart contracting, which is characterised by the use of pre-existing, externally developed code.

Despite these differences, a certain continuity between the two phenomena may still be identified. Both standard form contracts and smart contracts reduce the scope of negotiation and confine the parties' autonomy to a decision of acceptance or rejection. Yet, in smart contracts, this limitation is not merely economic or practical, but is embedded at the level of technical architecture. The contractual terms are not only pre-formulated, but are also encoded in such a way that their

⁴¹ Looney, J. W., *Adhesion Contracts, Bad Faith and Economically Faulty Contracts*, Drake Journal of Agricultural Law, pp. 177-195., available at: <https://aglawjournal.wp.drake.edu/wp-content/uploads/sites/66/2016/09/agVol04No1-Looney.pdf>, 25 February 2026.

execution is automatic and, in principle, resistant to modification or reinterpretation.

Accordingly, smart contracts may be understood not merely as a continuation of standard form contracting, but as its intensified and formalised manifestation. The restriction of contractual freedom shifts from the socio-economic sphere to the technological one: whereas classical adhesion contracts limit the formation of contractual will in an asymmetrical manner, smart contracts impose a structurally symmetrical and technologically enforced constraint that extends to both the formation and the execution of the contract.

This distinction is of fundamental importance for the assessment of freedom of contract in the digital environment. While both models reduce the scope of negotiation, only smart contracts eliminate, to a significant extent, the interpretative and corrective functions traditionally exercised by legal institutions. Consequently, smart contracts do not simply reproduce existing limitations of contractual autonomy, but transform them into a structurally embedded feature of the contractual mechanism itself.

The above comparative analysis demonstrates that, although smart contracts share certain structural similarities with classical standard form contracting, the nature of the constraints they impose differs in both origin and intensity. Building on this distinction, it becomes necessary to examine more closely how these technologically embedded limitations reshape the concept of contractual autonomy.

4.2. The Transformation of Contractual Autonomy under Smart Contracts

The three principal dimensions of classical freedom of contract – freedom to conclude a contract, freedom to choose one's contracting partner, and freedom to determine contractual content – are cast in a new light in the environment of smart contracts. Although, formally, the parties may still decide whether they wish to enter into a contract, the freedom to shape the content of the contract is essentially eliminated.

A smart contract operates on the basis of predetermined, coded conditions. The contractual declaration – unlike the classical declaration of intent – is not aimed at

the individual formulation of terms, but rather at their acceptance or rejection⁴². Consequently, autonomous decision-making is in fact reduced to a binary choice: to accept or to reject the algorithmic construction.

Within this digital contractual space, autonomy does not emerge as the result of free negotiation between the parties, but rather as the product of prior structuring through programming decisions. The technological environment – characterised by deterministic operation, full transparency, and traceability – displaces the traditional arenas of legal interpretation and contractual flexibility.

According to the principle of "code as law"⁴³, the regulatory function of law is, in part, performed by the programming itself. The smart contract is therefore not merely a legal act, but a technical structure whose execution does not require judicial involvement or legal interpretation. This represents a significant departure from the established system of continental private law, which is based on interpretation and on the balancing of the parties' interests.

The concept of digital determinism refers to the fact that contract execution proceeds according to predefined outcomes and leaves no room for context-sensitive decision-making. While this model enhances legal certainty and reduces the possibility of abuse, it simultaneously restricts precisely that sphere of individual decision-making which forms the foundation of freedom of contract in its classical sense.

Freedom of contract therefore does not disappear, but its meaning is transformed: from a classical legal principle it becomes a technologically determined entitlement, in which the parties' freedom extends only to initiating interaction. The possibility of negotiating and shaping the terms – constituting the core of private autonomy – is lost as a result of algorithmic contractual logic.

5. CONCLUSIONS

The aim of this study was to explore whether freedom of contract, as a classical legal principle, can prevail within the technological environment of smart contracts. The analysis has demonstrated that, in the continental private law

⁴² It is already a further question what type of conditions can be incorporated into smart contracts.

⁴³ De Filippi, P.; Hassan, S., *Blockchain Technology as a Regulatory Technology: From "Code Is Law" to "Law Is Code"*, available at: <https://arxiv.org/pdf/1801.02507>, 25 February 2026.

tradition, freedom of contract rests upon three pillars: freedom to conclude a contract, freedom to choose one's contracting partner, and freedom to determine the content of the contract. Of these three dimensions, smart contracts essentially leave only the first intact.

At the same time, the transformation identified in this study must be understood in a nuanced manner. On the one hand, smart contracts exhibit structural similarities with standard form and adhesion contracts, in which the parties' autonomy is likewise reduced to the acceptance or rejection of pre-formulated terms. On the other hand, however, smart contracts introduce a qualitatively new dimension of constraint, as the limitation of contractual freedom is no longer merely the result of economic or bargaining asymmetries, but is embedded in the technological architecture of the contractual mechanism itself.

The operation of smart contracts – pre-coded logic, automated execution, and a deterministic input–output relationship – creates a digital environment in which the role of the contracting parties is transformed: technical activation replaces autonomous decision-making. The parties do not negotiate or shape terms; rather, they accept them. Contractual intent is thus limited to affirming acceptance or rejecting entry.

At the same time, freedom of contract does not disappear, but its function becomes formalised: private autonomy is no longer expressed in the free determination of content, but merely in the binary decision to participate. According to the "code as law" approach, certain contractual norms are technologically determined, thereby narrowing the jurisprudential space for interpretation, balancing, and individual discretion.

In support of the study's hypothesis, it can be concluded that freedom of contract operates in a diminished form in the world of smart contracts. This limitation is not necessarily negative, since deterministic contracts may enhance legal certainty and reduce the possibility of abuse; nevertheless, from a legal-theoretical perspective, it is beyond doubt that the substantive sphere of individual autonomy is curtailed.

This insight may encourage future digital private law to reinterpret freedom of contract on new foundations, taking into account both the continuity with earlier forms of limited autonomy and the novel constraints arising from technological determinism, while preserving the requirements of fairness and balance between the parties.

REFERENCES

BOOKS AND ARTICLES

1. Béky, Á. E., *The Interpretation of Freedom of Contract in Modern Civil Law*, Debrecen, available at: <https://dea.lib.unideb.hu/server/api/core/bitstreams/a7787bc4-a990-4863-a2a9-d70bad5a31b4/content>, 25 February 2026.
2. Ben-Shahar, O., *Boilerplate and the Foundations of Contract Law*, Cambridge University Press, 2007, available at: https://assets.cambridge.org/97805216/76380/frontmatter/9780521676380_frontmatter.pdf, 25 February 2026.
3. Christidis, K.; Devetsikiotis, M., *Blockchains and Smart Contracts for the IoT*, Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC, USA 2016.
4. Csítei, B., *Smart Contracts*, Opuscula Civilia, 2019.
5. De Filippi, P.; Hassan, S., *Blockchain Technology as a Regulatory Technology: From "Code Is Law" to "Law Is Code"*, available at: <https://arxiv.org/pdf/1801.02507>, 25 February 2026.
6. European Law Institute, *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection*, European Union's Justice Programme, 2022, p. 25., available at: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf, 25 February 2026.
7. German, P., *What Is Proof of Stake and Proof of Work?*, CryptoFalka, available at: <https://cryptofalka.hu/proof-of-work-proof-of-stake/>, 25 February 2026.
8. Greenspan, G., *Avoiding the Pointless Blockchain Project*, 2015, available at: <https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/>, 25 February 2026.
9. Juhász, Á., *Online Contracting, Digital Content and Services, Smart Contracts – A New Era of Contract Law?*, Infocommunication and Law, 2020/2, (75.) e-special issue, available at: <https://infojog.hu/juhasz-agnes-online-szerzodeskotes-digitalis-tartalom-es-szolgaltatas-intelligens-szerzodesselel-a-szerzodesi-jog-uj-korszaka-2020-2-75-e-kulonszam/>, 25 February 2026.
10. Looney, J. W., *Adhesion Contracts, Bad Faith and Economically Faulty Contracts*, Drake Journal of Agricultural Law, available at: <https://aglawjournal.wp.drake.edu/wp->

content/uploads/sites/66/2016/09/agVol04No1-Looney.pdf, 25 February 2026.

11. Lyons, T.; Courcelas, L.; Timsit, K., *Legal and Regulatory Framework of Blockchains and Smart Contracts – A Thematic Report Prepared by the European Union Blockchain Observatory and Forum*, 27 September 2019.
12. Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, available at: <https://bitcoin.org/bitcoin.pdf>, 25 February 2026.
13. Szabó, G., *The Human Rights Risks of Globalisation*, PhD Dissertation, University of Pécs, Pécs 2008.
14. Szabo, N., *Smart Contracts*, 1994, available at: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>, 25 February 2026.
15. Szabo, N., *The Idea of Smart Contracts*, 1997, available at: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabs.best.vwh.net/idea.html>, 25 February 2026.
16. Szalai, Á., *The Content of the Contract*, Pázmány Law Working Papers, 2013/11.
17. Török, É., *Fundamental Issues of Contract Formation*, Debrecen 2013.
18. Waraich, R. S.; Fayaz, M.; Zahid, H., *Consent Theory and Adhesion Contract: A Critical Analysis of Contemporary Global Business Practices*, 2022, available at: https://www.researchgate.net/publication/365964837_Consent_Theory_and_Adhesion_Contract_A_Critical_Analysis_of_Contemporary_Global_Business_Practices, 25 February 2026.
19. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K., *Blockchain Technology Overview*, National Institute of Standards and Technology (NIST), 2018.

LEGAL ACTS

1. Civil Code, Act V of 2013 (Hungary).
2. Civil Code (Romania), Law No. 287/2009.

NETWORK RESOURCES

1. Buterin, V., *On Stake*, <https://blog.ethereum.org/2014/07/05/stake/>, 25 February 2026.

2. Mozilla Foundation, *How public key encryption works*, available at: <https://developer.mozilla.org/en-US/docs/>, 25 February 2026.
3. CoinCash, *What Is a Node?*, <https://hu.coincash.eu/kripto-szotar/n/node>, 25 February 2026.
4. TechTarget, *What Are the 4 Different Types of Blockchain Technology?*, <https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology>, 25 February 2026.

UDK: 366.5 (497.5 : 4-67 EU)
366.542 (497.5)(094.5)
Preliminary communication

Fani Milan Ostojić, PhD student
Faculty of Law, Unhiversity of Split, Croatia
E-mail: fani.milan.ostojic@pravst.hr
ORCID ID: 0000-0002-2368-2062

KEY CHARACTERISTICS OF THE DRAFT PROPOSAL FOR THE AMENDMENTS TO THE CONSUMER PROTECTION ACT OF 2025

ABSTRACT

On 22 December 2025, the Ministry of Economy of the Republic of Croatia submitted the Draft Proposal for the Amendments to the Consumer Protection Act to public e-consultation. The objectives of the draft are to enhance the level of consumer protection, provide a more detailed regulatory framework for traders' obligations, and increase the maximum amounts of regulatory fines. In addition to these objectives, the legislative initiative was motivated by the need to transpose into the Croatian legal system certain European Union directives. The paper provides a detailed analysis of the fundamental characteristics and the normative framework of the Draft Proposal, the reasons and objectives of the legislative intervention with particular emphasis on the aforementioned EU directives, as well as the anticipated legal implications for consumers' rights. Special attention is also given to the proposals and the final outcomes of the public e-consultation, which was concluded on 21 January 2026.

Keywords: *Consumer Protection; EU Directives; Consumer Protection Act; Amendments*

1. INTRODUCTION

Consumer protection law in the Republic of Croatia has developed, and continues to develop, under the strong influence of the European Union¹ law, within which consumer protection constitutes one of the most dynamic areas of regulation. Consumer protection policy is of particular importance for the functioning of the EU internal market. Accordingly, consumer protection law represents one of the so-called common policies of the EU, aimed at ensuring a high level of consumer protection in their relations with traders, with particular emphasis on vulnerable groups of consumers. The current objectives of the development of consumer

¹ Hereinafter referred to as: EU.

protection law in the EU include regulating the position of consumers in online marketplaces and promoting sustainable consumption within the framework of the circular economy.^{2,3} The objective of the Draft Proposal for the Amendments to the Consumer Protection Act of 2025⁴, for which the public e-consultation process was concluded on 21 January 2026, is to strengthen the position of consumers through clearer and more detailed regulation of pre-contractual information requirements, the regulation of price display provisions, the prohibition of unsolicited advertising materials, and the increase of regulatory fines for misdemeanours. Furthermore, the Draft Proposal seeks to further integrate Croatian consumer protection law into the EU consumer policy through the transposition of the relevant directives. These include Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC⁵; Directive (EU) 2024/825 of the European Parliament and of the Council of 28 February 2024 amending Directives 2005/29/EC and 2011/83/EU as regards empowering consumers for the green transition through enhanced protection against unfair commercial practices and improved information requirements⁶; and Directive (EU) 2024/1799 of the European Parliament and of the Council of 13 June 2024 on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394 and Directives (EU) 2019/771 and (EU) 2020/1828⁷. By transposing the aforementioned Directives into the Consumer Protection Act, Croatian consumer protection law will be further aligned with the evolving EU *acquis*, thereby reinforcing legal certainty, enhancing the level of consumer protection, and ensuring the effective functioning of the internal market. In the first part of the paper, the development and current state of consumer protection law in the Republic of Croatia will be analysed, together with the identification of key challenges faced by consumers in the exercise of their rights, as well as areas

² In more detail see: Mišćenić, E., *Sustainability, the Circular Economy and Consumer Law in Croatia*, Journal of European Consumer and Market Law, vol. 9., no. 4/2020, pp. 173–176.

³ Ministry of Economy, National Consumer Protection Programme for the period until 2028, Zagreb, July 2025., <https://mingo.gov.hr/UserDocImages/slike/Vijesti/2022/Nacionalni%20program%20za%20C5%A1tite%20potro%C5%A1a%C4%8Da%20za%20razdoblje%20do%202028..pdf>, 16 February 2026 (hereinafter referred to as: NCPP).

⁴ Hereinafter referred to as: Draft Proposal.

⁵ Official Journal of the European Union L 2023/2673, 28.11.2023 (hereinafter referred to as: Directive (EU) 2023/2673)

⁶ Official Journal of the European Union L 2024/825, 6.3.2024 (hereinafter referred to as: Directive (EU) 2024/825)

⁷ Official Journal of the European Union L 2024/1799, 10.7.2024. (hereinafter referred to as: Directive (EU) 2024/1799)

requiring further improvement, based on case law. Subsequently, the current state of consumer protection law in the European Union will be presented, with particular emphasis on directives that are implemented into Croatian consumer protection law through amendments to the Consumer Protection Act. After a detailed review of the amendments to the Consumer Protection Act introduced by the Draft Proposal, the proposals and final results of the conducted e-Consultation will be presented, and the implications of the proposed changes for the position of consumers will be discussed, with particular emphasis on whether the identified problems in the enforcement of consumer rights in the Republic of Croatia are addressed by the proposed amendments and whether they strengthen the legislative framework of consumer protection in the areas where this is necessary.

2. PREVIOUS DEVELOPMENT AND THE CURRENT STATE OF CONSUMER PROTECTION LAW IN THE REPUBLIC OF CROATIA

2.1. Development and Primary Sources of Consumer Protection Law in the Republic of Croatia

Consumer Protection Law in the Republic of Croatia⁸, in terms of the existence of a systematic framework for the protection of consumer rights that promotes transparency, regulates contractual terms, ensures consumer information, supports consumer protection associations and organizations, and enhances safety standards and the quality of goods⁹, began to develop more substantially with the initiation of the process of accession to the EU, namely with the signing of the

⁸ For an overview of consumer protection law in the Republic of Croatia see: Baretić, M., *Zaštita potrošača u Republici Hrvatskoj nakon ulaska u Europsku uniju: jesmo li implementacijom europskog prava izgradili sustav zaštite potrošača?*, in: Bourgoignie, T.; Jovanović, T. (eds.), *Strengthening Consumer Protection in Serbia: Liber Amicorum Svetislav Taborši*, Pravni fakultet Univerziteta u Beogradu, Beograd 2013., pp. 65–112.; Salač, J.; Uzelac, J., *Zaštita potrošača u Republici Hrvatskoj u kontekstu harmonizacije s pravnom stečevinom Europske unije*, FIP - Financije i pravo, vol. 2, no. 2/2014, pp. 7–27.; Baretić, M., *Individualna i kolektivna zaštita potrošača u hrvatskom pravu*, in: Tomljenović, V.; Čulinović Herc, E.; Butorac Malnar, V. (eds.), *Republika Hrvatska na putu prema Europskom pravosuđnom području – rješavanje trgovačkih i potrošačkih sporova*, Pravni fakultet Sveučilišta u Rijeci, Rijeka 2009., pp. 241–286.; Mišćenić, E., *Usklađivanje prava zaštite potrošača u Republici Hrvatskoj*, Godišnjak Akademije pravnih znanosti Hrvatske, vol. IV, no. 1/2013., pp. 145–176.

⁹ Babić, M., *Zaštita prava potrošača i izvori trgovačkog prava*, Poslovna izvrsnost, vol. IX, No. 1/2015., p. 75.

Stabilisation and Association Agreement¹⁰ in 2001. Under the said Agreement, the Republic of Croatia undertook to harmonise its existing and future legislation with the *acquis communautaire* of the European Community, with the alignment in the initial phase to focus on the fundamental components of the *acquis*, including consumer protection law.¹¹ The first Croatian Consumer Protection Act¹², by which the *acquis communautaire* in the field of consumer protection law¹³ was transposed into the Croatian national legal system, was adopted in 2003, while the first National Consumer Protection Programme was enacted at the beginning of 2005.¹⁴ However, this does not mean that, prior to the signing of the Stabilisation and Association Agreement, Croatian legislation did not contain provisions which, within both public law and private law frameworks, afforded protection to consumer rights. Thus, already within the framework of the Socialist Federal Republic of Yugoslavia¹⁵, the rules of the General Customs for Trade of Goods¹⁶ and the Fundamental Act on the Trade of Goods¹⁷ provided, in cases of delivery of defective goods, for the buyer's rights to require the removal of defects, replacement of defective goods with conforming goods, and withdrawal from the contract.¹⁸ In addition to the aforementioned rights, the General Customs also provided for the possibility of a reduction of the purchase price, a remedy which, however, was not recognised under the Fundamental Act on the Trade of Goods.¹⁹ Provisions relevant to the position of consumers were also contained in the Civil

¹⁰ Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Croatia, of the other part, Official Gazette – International Treaties no. 14-132/0 (hereinafter referred to as: Stabilisation and Association Agreement)

¹¹ Mišćenić, E., *Usklađivanje prava zaštite potrošača...*, *op. cit.* in fn. 8, p. 146.

¹² Consumer Protection Act, Official Gazette No. 96/2003, 46/2007, 79/2007. To date, three additional Consumer Protection Acts have been adopted: in 2007 (Official Gazette, No. 79/2007, 125/2007, 79/2009, 89/2009, 75/2009, 133/2009, 78/2012, 56/2013, 41/2014), in 2014 (Official Gazette, No. 41/2014, 110/2015, 14/2019, 19/2022), and, currently in force, in 2022 (Official Gazette, No. 19/2022, 59/2023; hereinafter referred to as: CPA).

¹³ Babić, M., *op. cit.* in fn. 9, p. 75.

¹⁴ National Consumer Protection Programme for the period 2005. – 2006. of 25 February 2005., https://www.hah.hr/pdf/program_zastite_potrosaca.pdf, 12 February 2026.

¹⁵ Hereinafter referred to as: SFRY.

¹⁶ Official Gazette of the FNRJ No. 15/1954, Official Gazette of the SFRY No. 29/1978, Official Gazette No. 53/1991, 35/2005 (hereinafter referred to as: General Customs).

¹⁷ Official Gazette of the SFRY, No.1/1967 (hereinafter referred to as: Fundamental Act on the Trade of Goods).

¹⁸ See: Josipović, T., *Das Konsumentenschutzgesetz – Beginn der Europäisierung des kroatischen Vertragsrechts*, in: Grundmann, S.; Schauer, M. (eds.), *The Architecture of European Codes and Contract Law*, Kluwer Law International, Vienna 2006., p. 141.

¹⁹ Ledić, D., *Consumer Protection Law – A Separate Branch of the New Croatian Legal System*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 13., no. 1/1992., pp. 149–150.

Obligations Act of 1978²⁰, which, in Article 8, regulated obligations toward citizens as consumers and users of services²¹, and in Article 9, established the principle prohibiting harm to consumers and other market participants²². Furthermore, the provisions of the COA/78 concerning the sale with installment payments²³ applied only in transactions involving an "individual buyer"²⁴ and contained rights that coincided with those protected under consumer protection law.²⁵ However, in principle, the COA/78 did not explicitly contain provisions aimed at protecting consumer rights; rather, it safeguarded consumers in the same manner as it has protected any other party in an obligation relationship.²⁶ After the Republic of Croatia has gained independence in 1991, the COA/78 was incorporated into the Croatian legal system through the Act on the Adoption of the Civil Obligations Act²⁷, where it functioned as the primary source of obligations law, including contract law, until the entry into force of the current Civil Obligations Act²⁸ on 1 January 2006.²⁹ Following the signing of the Stabilisation and Association Agreement, at a time when, for the purpose of fulfilling the obligations to harmonise Croatian legislation with the European Community *acquis*³⁰, EU directives on the protection of consumer rights were to be incorporated into the Croatian legal system³¹, the Croatian legislator decided to achieve this by enacting the aforementioned Consumer Protection Act of 2003.³² This approach was intended to preserve the systematic coherence and consistency

²⁰ Civil Obligations Act, Official Gazette of the SFRY No. 29/1978, 39/1985, 46/1985, 57/1989, Official Gazette No. 53/1991, 73/1991, 3/1994, 111/1993, 107/1995, 7/1996, 91/1996, 112/1999, 88/2001, 35/2005 (hereinafter referred to as: COA/78).

²¹ See: COA/78, Art. 8.

²² See: COA/78, Art. 9.

²³ See: COA/78, Art. 542. – 551.

²⁴ COA/78, Art. 542. para. 2.: The rules contained in this section concerning the sale of goods on installment terms shall apply exclusively where the buyer is an individual.

²⁵ Thus, the provision of Art. 544, para. 2 of the COA/78 established the right of an individual buyer to withdraw from the contract within three days of signing the document, a right from which the buyer could not waive. Art. 545 of the COA/78 stipulated that the buyer may at any time pay off the remaining balance in full, while Art. 551 of the COA/78 provided for the nullity of any contractual provisions on installment payments that would be less favorable to the buyer than the applicable provisions of the COA/78, and others.

²⁶ Čikara, E., *Hrvatska – zakonodavne tehnike*, in: Jessel-Holst, C.; Galev, G. (eds.), *EU Consumer Contract Law; Potrošačko ugovorno pravo Evropske unije*, Civil Law Forum for South East Europe Collection of Studies and Analyses, vol. III, Beograd-Zagreb 2010., pp. 592–595.

²⁷ Act on the Adoption of the Civil Obligations Act, Official Gazette No. 53/1991

²⁸ Civil Obligations Act, Official Gazette No. 35/2005, 41/2008, 125/2011, 78/2015, 29/2018, 126/2021, 114/2022, 156/2022, 145/2023, 155/2023 (hereinafter referred to as: COA).

²⁹ See: Salač, J.; Uzelac, J., *op. cit.* in fn. 8, p. 13.

³⁰ See: *supra*, p. 3.

³¹ See: Mišćenić, E., *Usklađivanje prava zaštite potrošača...*, *op. cit.* in fn. 8, p. 147.

³² See: *supra*, p. 3.

of the COA/78, as the latter was terminologically inconsistent with the EU directives, which primarily pursue the economic objective of establishing and functioning of the single market.³³ However, when it became necessary to implement Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees³⁴ into Croatian legislation, the legislator followed the German model, essentially implementing it through the enactment of, and subsequent amendments to, the COA³⁵, while only partially incorporating it into the 2003 Consumer Protection Act.³⁶ The objectives of Directive 1999/44/EC of the European Parliament and of the Council were reflected in Articles 400–429 of the COA, which addressed liability for material defects, and in Articles 430–437, which governed liability for legal defects.³⁷ In the same manner, the Council Directive of 25 July 1985 on the approximation of the laws and regulations of the Member States concerning liability for defective products³⁸ was also transposed into the 2005 COA.³⁹ As a result, the COA became the second most important legal act in the Republic of Croatia regarding the protection of consumer rights, with the CPA serving as the *lex specialis* and the COA as the *lex generalis*, as explicitly stipulated in Article 3 of the CPA.⁴⁰ In the same manner, the Directive (EU) 2019/771 of the European Parliament and of the Council on certain aspects of contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC⁴¹, was essentially

³³ Mišćenić, E., *Usklađivanje prava zaštite potrošača...*, *op. cit.* in fn. 8, p. 147.

³⁴ Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, Official Journal of the European Communities, L 171, 07 July 1999 (hereinafter referred to as: Directive 1999/44/EC)

³⁵ See: Act on Amendments to the Civil Obligations Act, Official Gazette No. 78/2015, Art. 1a

³⁶ Jokanović, I.; Dudás, A., *Lack of Conformity and Seller's Liability in Croatian, Slovenian and Serbian Law*, Zbornik Pravnog fakulteta u Zagrebu, vol. 75, no. 4/2025, p. 553.

³⁷ See in detail in: Kanceljak, I., *Reform of Consumer Sales Law of Goods and Associated Guarantees – Possible Impact on Croatian Private Law*, EU and Comparative Law Issues and Challenges Series (ECLIC), vol. 2/2018: EU Law in Context – Adjustment to Membership and Challenges of the Enlargement, University Josip Juraj Strossmayer of Osijek, Faculty of Law Osijek, pp. 586–610.

³⁸ Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), Official Journal of the European Communities, L 210, 7 August 1985

³⁹ See: Act on Amendments to the Obligations Act, Official Gazette No. 78/2015, Art. 1a

⁴⁰ CPA, Art. 3. para. 2.: Unless otherwise provided by the special laws referred to in paragraph 1 of this Article or by this Act, the provisions governing obligations shall apply to contractual relationships between consumers and traders.

⁴¹ Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, Official

transposed through amendments to the provisions on liability for material defects and guarantees in the COA.⁴² This legislative adaptation provided an even higher level of consumer protection, since Directive (EU) 2019/771, unlike its predecessor Directive 1999/44/EC, is a directive of maximum harmonisation, aimed at removing barriers to cross-border trade by enhancing consumer rights through additional regulation of product conformity, consumer rights in cases of non-conformity, and the means to enforce those rights.⁴³ On the other hand, the Consumer Protection Acts incorporated Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts⁴⁴, Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of prices of products offered to consumers⁴⁵, Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council, and repealing Council Directives 85/577/EEC and 97/7/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 on unfair business-to-consumer commercial practices⁴⁶, Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 on distance marketing of consumer financial services, amending Council Directive 90/619/EEC, and Directives 97/7/EC and 98/27/EC⁴⁷, among others.⁴⁸ From all of the above, it is clear that consumer protection law in the Republic of Croatia is not organised in a unified and systematic manner, but is rather characterised by a fragmented regulatory framework.⁴⁹ In addition to the aforementioned Consumer

Journal of the European Union, L 136, 22 May 2019 (hereinafter referred to as: Directive (EU) 2019/771)

⁴² See: Act on Amendments to the Civil Obligations Act, Official Gazette No. 126/2021

⁴³ See: Kanceljak, I., *Reform of Consumer Sales Law...*, *op. cit.* in fn. 37, pp. 594, 606 *et seq.*

⁴⁴ Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, Official Journal of the European Communities, L 95, 21 April 1993

⁴⁵ Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers, Official Journal of the European Communities, L 80, 18 March 1998

⁴⁶ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), Official Journal of the European Union, L 149, 11 June 2005

⁴⁷ Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC, Official Journal of the European Communities, L 271, 09 October 2002

⁴⁸ See: CPA. Art. 2.

⁴⁹ Mišćenić, E., *Usklađivanje prava zaštite potrošača...*, *op. cit.* in fn. 8, p. 149.

Protection CPA and the COA, which constitute the foundational pillars of consumer protection law in Croatia, other significant legal sources include the Act on Certain Aspects of Contracts for the Supply of Digital Content and Digital Services⁵⁰, the Act on Unfair Advertising⁵¹, the Act on Representative Actions for the Protection of Collective Interests and Consumer Rights⁵², the Act on Alternative Dispute Resolution in Consumer Matters⁵³, among others. The perception of fragmentation in this area of law is further reinforced by the frequent amendments to the relevant legislation, particularly the CPA⁵⁴, which are driven by the need to continuously align Croatian consumer law with the EU *acquis* in this field—one of the most dynamic areas of Community law.⁵⁵

2.2. Current State and Challenges of Consumer Protection Law in the Republic of Croatia - Legislative Framework and Case Law Review

2.2.1. On the Current CPA as *lex specialis* of the Consumer Protection Law in the Republic of Croatia

The currently applicable CPA, serving as the primary legal source and *lex specialis* in the field of consumer protection law in the Republic of Croatia, was enacted in 2022.⁵⁶ Through this Act, Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019, amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC, and 2011/83/EU of the European Parliament and of the Council to improve the enforcement and modernisation of Union consumer protection rules⁵⁷—commonly referred to as the „Omnibus Directive“—was implemented into Croatian legislation. The Directive aims to modernise and enhance rules on consumer protection and information in line with market

⁵⁰ Official Gazette No. 110/2021

⁵¹ Official Gazette No. 43/2009

⁵² Official Gazette No. 59/2023

⁵³ Official Gazette No. 121/2016, 32/2019

⁵⁴ It should be recalled that since the signing of the Stabilisation and Association Agreement, which marked the beginning of a period of intensive development of consumer protection law in the Republic of Croatia, no fewer than four separate Consumer Protection Acts have been enacted, each of which has been amended and supplemented a significant number of times. See *supra*, note 12.

⁵⁵ See: Mišćenić, E., *Usklađivanje prava zaštite potrošača...*, *op. cit.* in fn. 8, pp. 148–149.

⁵⁶ See *supra*, note 12. The CPA entered into force on 28 May 2022.

⁵⁷ Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, Official Journal of the European Union, L 328, 18 December 2019

developments, with particular focus on regulating the relationship between sellers and buyers in the context of online commerce. Compared to the previous legislation, the CPA, in the context of seasonal sales, promotional campaigns, clearance sales, and sales of defective goods, introduced the obligation for traders to display the lowest price of a product over the preceding 30 days⁵⁸, as well as to inform the consumer if the retail price of a product is determined on a personalised basis through an automated decision-making system.⁵⁹ Additional transparency requirements were also introduced for online marketplaces, for example regarding whether the party offering products on the platform is a trader⁶⁰.⁶¹ In July 2025, a new National Consumer Protection Programme for the period until 2028⁶² was adopted, setting as its general objective the empowerment of consumers to become active and resilient participants in the dynamic global market, contribute to Croatia's sustainable circular economy, and effectively utilise national mechanisms for the protection of their rights, including provisions adapted for the most vulnerable social groups.⁶³ Among the specific objectives and measures, the first is the continuous development of legislation in the field of consumer protection, with the initial measure being precisely the adoption of amendments to the CPA and other related regulations. Through these amendments, the relevant EU directives in the area of consumer protection law are also planned to be transposed into Croatian legislation.⁶⁴

2.2.2. Consumer Protection in the Republic of Croatia: Case Law and Identified Challenges

The effectiveness of the implementation of EU consumer protection policy in the Republic of Croatia, as well as its overall development, does not depend solely on the successful transposition of EU legislation into national law, but also on the

⁵⁸ CPA, Art. 19. para. 4.

⁵⁹ CPA, Art. 90. para. 1. point 6.

⁶⁰ CPA, Art. 36. para. 4. point 6.

⁶¹ See: Dabović Anastasovska, J., *Implementacija novina potrošačkog prava Europske unije u potrošačke zakone zemalja regije*, Zbornik radova građanskog i trgovačkog zakonodavstva i pravne prakse, no. 20., Mostar 2023., pp. 24–25.

⁶² NCPP.

⁶³ See: *Ibid.*, p. 11.

⁶⁴ See: *Ibid.*, pp. 11–13. Among other specific objectives set out in the NCPP are the improvement of mechanisms for out-of-court resolution of consumer disputes, strengthening market surveillance mechanisms for the protection of consumers, informing and raising awareness of consumer rights, creating conditions for sustainable and circular consumption, mitigating the social effects of inflation, enhancing the general safety system for non-food products and consumer information on food, improving consumer protection in the digital environment and the development of digital tools for consumers, as well as international cooperation in consumer protection. See *Ibid.*, pp. 14 *et seq.*

establishment of an adequate administrative structure, the development of institutional capacities and enforcement mechanisms, the level of cooperation and capacities of consumer protection associations, and effective oversight of policy implementation, including both out-of-court and judicial mechanisms for resolving consumer disputes.⁶⁵ Within the framework of procedural consumer protection in the Republic of Croatia, in addition to the possibility of protection through proceedings initiated by individual actions in accordance with the provisions of the Civil Procedure Act⁶⁶, the CPA in Part IV, Chapter I, regulates alternative consumer dispute resolution, while Chapter II governs the protection of the collective interests and rights of consumers.⁶⁷ Alternative dispute resolution (ADR) in consumer matters refers to the out-of-court settlement of disputes between traders and consumers⁶⁸, whereas the mechanism of collective legal protection is aimed at seeking the cessation of conduct by the defendant that is contrary to consumer protection regulations, the adoption of measures to eliminate harmful consequences, and the prohibition of such and similar conduct in the

⁶⁵ See: *Ibid.*, p. 10. See: *Ibid.*, p. 10.

⁶⁶ Official Gazette of the SFRY No. 4/1977, 36/1977, 36/1980, 6/1980, 69/1982, 43/1982, 58/1984, 74/1987, 57/1989, 20/1990, 27/1990, 35/1991, Official Gazette of the Republic of Croatia No. 53/1991, 91/1992, 112/1999, 129/2000, 88/2001, 117/2003, 88/2005, 2/2007, 96/2008, 84/2008, 123/2008, 57/2011, 25/2013, 89/2014, 70/2019, 80/2022, 114/2022, 155/2023, 146/2025

⁶⁷ See: CPA, Part IV, Chapters I. and II.

⁶⁸ On alternative dispute resolution in consumer matters, see in detail in: Tepeš, N., *Izvensudsko rješavanje potrošačkih sporova u Hrvatskoj*, in: Tomljenović, V.; Čulinović Herc, E.; Butorac Malnar, V., *Republika Hrvatska na putu prema Europskom pravosuđnom području: Rješavanje trgovačkih i potrošačkih sporova*, Pravni fakultet Sveučilišta u Rijeci, Rijeka, 2009., p. 171. – 200., Poretti, P., P., *Sudska zaštita prava potrošača – (naj)bolji put?*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39., no. 1/2018, pp. 537. – 549., Petrašević, T.; Poretti, P., *Consumer Protection in Croatia with a Special Emphasis on Distance and off-Premises Contracts*, Journal for Legal Theory and Practice, Vol. 3., No. 1., 2016., pp. 31. – 41., Proso, M.; Milan Ostojić, F., *Zaštita (kolektivnih) interesa i prava potrošača i alternativno rješavanje potrošačkih sporova*, Zbornik radova IX. međunarodnog savjetovanja „Aktualnosti građanskog procesnog prava – nacionalna i usporedna pravnoteorijska i praktična dostignuća“, Split, 2023., pp. 173. – 196. For a detailed comparison of the consumer protection system see: Tepeš, N., *Izvensudsko rješavanje potrošačkih sporova u Hrvatskoj*, in: Tomljenović, V.; Čulinović Herc, E.; Butorac Malnar, V. (eds.), *Republika Hrvatska na putu prema Europskom pravosuđnom području: Rješavanje trgovačkih i potrošačkih sporova*, Pravni fakultet Sveučilišta u Rijeci, Rijeka 2009., pp. 171–200.; Poretti, P., *Sudska zaštita prava potrošača – (naj)bolji put?*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39., no. 1/2018, pp. 537–549.; Petrašević, T.; Poretti, P., *Consumer Protection in Croatia with a Special Emphasis on Distance and off-Premises Contracts*, Journal for Legal Theory and Practice, Vol. 3., No. 1/2016., pp. 31–41.; Proso, M.; Milan Ostojić, F., *Zaštita (kolektivnih) interesa i prava potrošača i alternativno rješavanje potrošačkih sporova*, Zbornik radova IX. međunarodnog savjetovanja „Aktualnosti građanskog procesnog prava – nacionalna i usporedna pravnoteorijska i praktična dostignuća“, Split 2023., pp. 173–196.

future⁶⁹. In the development of the collective redress mechanism in the Republic of Croatia, the case law of the Supreme Court of the Republic of Croatia in the "Franak" case has had a particularly significant influence, as it was the first collective consumer protection case in Croatia following the introduction of this mechanism in 2003.⁷⁰ Despite the existence of these procedural mechanisms, consumer protection in the Republic of Croatia is, in practice, not at a satisfactory level. There is a lack of case law in the application of the provisions of the Consumer Protection Act (CPA)⁷¹, and scholarly literature identifies as one of the reasons the fact that courts often protect consumers in the same manner as any other party, thereby disregarding the specific provisions on consumer protection.⁷² In addition, the limited case law on the application of the CPA can also be attributed to a general reluctance of consumers to seek judicial protection of their rights.⁷³ Among the available case law, particular mention should be made of that

⁶⁹ A consumer may seek compensation for damages only in subsequently initiated individual court proceedings, relying on a decision rendered in collective consumer protection proceedings. On collective legal protection see in detail in: Poretti, P., *op.cit.*, note 68., pp. 549. - 553., Maganić, A., *Predstavničke tužbe za zaštitu kolektivnih interesa i prava potrošača u Republici Hrvatskoj*, Zbornik radova „Aktualnosti građanskog i trgovačkog zakonodavstva i pravne prakse“, no. 20., Mostar, 2023., pp. 146. – 161. See: Poretti, P., *op. cit.* in fn. 68, pp. 549–553.; Maganić, A., *Predstavničke tužbe za zaštitu kolektivnih interesa i prava potrošača u Republici Hrvatskoj*, Zbornik radova „Aktualnosti građanskog i trgovačkog zakonodavstva i pravne prakse“, no. 20., Mostar 2023., pp. 146–161.

⁷⁰ See: Mišćenić, E., *Croatian Case "Franak": Effective or "Defective" Protection of Consumer Rights?*, *Harmonius: Journal of Legal and Social Studies in South East Europe*, 2016., pp. 184. – 209. and the decision of the Supreme Court of the Republic of Croatia, case no. Revt-575/2016-5 of 3 October 2017. See: Mišćenić, E., *Croatian Case „Franak“: Effective or „Defective“ Protection of Consumer Rights?*, *Harmonius: Journal of Legal and Social Studies in South East Europe*, 2016., pp. 184–209.

⁷¹ According to data available on the www.iusinfo.hr portal, the largest number of available decisions of the Supreme Court of the Republic of Croatia, which predominantly relate to judgments in individual cases initiated on the basis of the "Franak" case, amounts to a total of 221. There are 55 decisions of the High Misdemeanour Court of the Republic of Croatia, 36 decisions of the High Commercial Court, 32 decisions of the Constitutional Court of the Republic of Croatia, and only 23 decisions of county courts. See: <https://www.iusinfo.hr/zakonodavstvo/ZA2022B19A203>, Accessed 25 March 2026.

⁷² See: Mišćenić, E., *Usklađivanje prava zaštite potrošača u Republici Hrvatskoj*, *op.cit.*, note 8., p. 167. See: Mišćenić, E., *Usklađivanje prava zaštite potrošača...*, *op. cit.* in fn. 8, p. 167.

⁷³ At the EU level, according to the 2025 Consumer Conditions Scoreboard, in 2024, in the event of a problem, 73% of consumers took some form of action, while 27% did not attempt to resolve the issue at all. Among those who took action, 85% addressed the problem directly to the trader, while only 5% sought judicial protection. The situation regarding alternative dispute resolution (ADR) is not significantly better, as only 9% of consumers resorted to it. See: 2025 Consumer Conditions Scoreboard, https://commission.europa.eu/document/download/2816337b-4fd1-4db2-a71c-d14a206a5a93_en?filename=consumer_conditions_scoreboard_2025_final.pdf, Accessed 25 March 2026.

of the Supreme Court of the Republic of Croatia in proceedings based on the "Franak" case, concerning unfair terms in consumer contracts, the case law of the Constitutional Court of the Republic of Croatia relating to the conclusion of distance consumer contracts⁷⁴ and decisions concerning the obligation to make product information available and to display product declarations.⁷⁵

Particular attention should be given, in terms of volume, to decisions rendered in misdemeanour proceedings concerning violations of the provisions of the CPA, as these potentially point to certain deficiencies in the legal framework in ensuring the effective enforcement of the Act. A large number of decisions have thus been rendered in misdemeanour proceedings concerning the use of prohibited (unfair, misleading, or aggressive) commercial practices⁷⁶, while in the majority of cases the regulatory fines were set at the lower end of the statutory range⁷⁷, with the possibility of mitigating the penalty being applied in a considerable number of cases as well.⁷⁸ The large number of such cases in case law, together with the fact that defendants are often legal persons—frequently large retail chains that in some instances appear as defendants in multiple proceedings due to repeated infringements⁷⁹—and taking into account the sanctions imposed, leads to the

⁷⁴ See the decisions of the Constitutional Court of the Republic of Croatia case no. Usl-4002/13-11 of 3 June 2015., Usl-3562/13-10 of 27 August 2015., Usl-1106/14-9 of 27 April 2016. and Usl-4304/13-8 of 9 September 2015.

⁷⁵ See the holding of the High Misdemeanour Court of the Republic of Croatia in case No. Gž-6360/10 of 24 April 2013, as well as that court's decisions Nos. Gž-5044/11 of 16 April 2014 and Gž-5713/2011 of 24 October 2014.

⁷⁶ See the decisions of the High Misdemeanour Court of the Republic of Croatia no. Ppž-7929/2024-2 of 20 February 2025, Ppž-2213/2025-2 of 26 November 2025, Gž-1263/2019-2 of 29 September 2021, Gž-129/2019 of 2 November 2021, Gž-50/2019 of 6 March 2019, Gž-1064/2018 of 10 April 2019, Ppž-6262/2025-2 of 15 July 2025, Ppž-13024/2022-2 of 15 July 2025, and the decision of the Municipal Court in Novi Zagreb no. Pp-81/2023-24 of 22 March 2024.

⁷⁷ Under Article 138 of the Consumer Protection Act of 2014, fines for misdemeanours arising from breaches of the provisions of that Act were set in the range of HRK 10,000.00 to 100,000.00 for legal persons, and HRK 10,000.00 to 15,000.00 for responsible persons. Under Article 149 of the currently applicable CPA, fines are prescribed in the amount ranging from HRK 10,000.00 to 200,000.00 for legal persons, and HRK 10,000.00 to 15,000.00 for responsible persons.

⁷⁸ Thus, for example, in the decision of the High Misdemeanour Court No. Gž-129/2019 of 2 November 2021, a fine of HRK 5,000.00 was imposed on the legal person and HRK 3,000.00 on the responsible person; in the judgment of the same court No. Ppž-7929/2024-2 of 20 February 2025, fines in the amount of EUR 1,327.00 were imposed on both the legal and the responsible person; and in the judgment of the same court No. Ppž-2213/2025-2 of 26 November 2025, a fine of EUR 3,000.00 was imposed on the legal person and EUR 1,500.00 on the responsible person, etc.

⁷⁹ As is the case in the decisions of the High Misdemeanour Court of the Republic of Croatia No. Ppž-2213/2025-2 of 26 November 2025, No. Ppž-7929/2024-3 of 20 February 2025,

conclusion that the prescribed and imposed penalties for violations of the CPA do not have a sufficient deterrent effect to discourage potential offenders from non-compliance with its provisions. It is therefore argued that, *de lege ferenda*, the introduction of more robust enforcement mechanisms against traders in cases of consumer law infringements is necessary. Given that the Draft Proposal foresees amendments to the existing framework of misdemeanour penalties for violations of the CPA, the analysis of these amendments will seek to assess whether they adequately address the identified issues of insufficient deterrence and enforcement effectiveness highlighted in case law.

3. REASONS AND OBJECTIVES OF LEGISLATIVE INTERVENTION – EU DIRECTIVES

3.1. On the Development of Consumer Protection Law in the EU

Consumer protection law within the EU developed, on the one hand, as an integral part of measures aimed at improving the functioning of the internal market and harmonising legislation, and on the other hand, as a response to the recognised need to protect consumer rights as a socio-political objective.⁸⁰ The origins of this area within the EU date back to the 1970s, when the Council of the European Economic Communities adopted a Preliminary Programme for Consumer Protection and Information Policy⁸¹ in 1975. This Programme established the fundamental consumer rights: the right to protection of health and safety, the right to protection of economic interests, the right to redress, the right to information and education, and the right to representation (the right to be heard).⁸² The most significant development in consumer protection was the entry into force of the Treaty on European Union⁸³ in 1993. For the first time, consumer protection was recognised as an independent policy of the European Community, with a dedicated

and No. Ppž-13024/2022-2 of 15 July 2025, in which proceedings were conducted against the defendant Plodine d.d. concerning various forms of prohibited commercial practices.

⁸⁰ Poretti, P., *op. cit.* in fn. 68, p. 536.

⁸¹ Council Resolution of 14 April 1975 on a preliminary programme of the European Economic Community for a consumer protection and information policy, Official Journal of the European Communities, C 92, 25 April 1975

⁸² See: Sukačić, M., *European Consumer in Sales Contract – the Ancient Approach, De Lege Lata & De Lege Ferenda*, EU and Comparative Law Issues and Challenges Series (ECLIC), no. 8., 2024., p. 874.

⁸³ Treaty on European Union, Official Journal of the European Communities, C 191, 29 July 1992 (known as and hereinafter regarded to as: Maastricht Treaty)

chapter entitled "Consumer Protection"⁸⁴ assigned to this area.⁸⁵ The adoption of the Maastricht Treaty marked the shift from non-binding, *soft law* in consumer protection to the conferral of legislative powers on the Community in this field. Consequently, the Community's competences in consumer protection were expanded, although they remained limited by the principle of subsidiarity, granting the Community the authority to act only where the objectives could not be sufficiently achieved by the Member States themselves.⁸⁶ Building on the aforementioned developments, the field of consumer protection within the EU is characterised by rapid evolution and growing significance. The Consumer Protection Strategy for the period 2002–2006 introduced the principle of maximum harmonisation, which does not permit any deviation from the provisions of directives during their implementation.⁸⁷ Equally important for the alignment of legal regulations in the field of consumer protection is the principle of so-called targeted full harmonisation, whereby national legislators are not allowed to retain existing or adopt new legal provisions that diverge from the directives, except where the directives themselves explicitly allow such deviations.⁸⁸ Furthermore, a high level of consumer protection has been established as an integral part of EU policy by the Charter of Fundamental Rights of the European Union^{89,90}. Since the entry into force of the Lisbon Treaty⁹¹ in 2007, the rights, freedoms, and principles enshrined in the Charter have acquired the same legal force as the provisions of the Founding Treaties⁹², thereby unequivocally recognising consumer protection as one of the fundamental and most important objectives of the EU. Today, the legal foundation of consumer protection in the EU consists, in addition to Article 38 of the Charter of Fundamental Rights, of the relevant provisions of the Treaty

⁸⁴ Maastricht Treaty, Art. 129a

⁸⁵ Pošćić, A., *Europsko pravo tržišnog natjecanja i interesi potrošača*, Narodne novine, Zagreb 2014., pp. 13–14.

⁸⁶ Weatherhill, S., *EU Consumer Law and Policy*, Edward Elgar Publishing Ltd, Cheltenham; Northampton 2005., p. 19.

⁸⁷ On the principle of maximum harmonisation, see: Mišćenić, E., *Europsko privatno pravo, opći dio*, Školska knjiga, Zagreb 2019., pp. 98–100.

⁸⁸ See: Mišćenić, E., *Usklađivanje prava zaštite potrošača...*, *op. cit.* in fn. 8, p. 152.

⁸⁹ Charter of Fundamental Rights of the European Union, Official Journal of the European Communities C 364/1, 18.12.2000 (hereinafter referred to as: Charter of Fundamental Rights of the European Union)

⁹⁰ Charter of Fundamental Rights of the European Union, Art. 38.: Union policies shall ensure a high level of consumer protection.

⁹¹ Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, Official Journal of the European Union, C 306, 17 December 2007 (hereinafter referred to as: Treaty of Lisbon)

⁹² Treaty of Lisbon, Art. 6.

on the Functioning of the European Union⁹³, which define the competences, objectives, and procedures of the Union in this field.

3.2. Current State of EU Consumer Protection Legislation and Key Characteristics of the Directives Relevant to Amendments to the Consumer Protection Act

In its 2025 Work Programme, the European Commission presented the Consumer Agenda for the period 2025–2030⁹⁴, which was adopted on 19 November 2025. The adoption of the new Consumer Protection Strategy followed five years after the adoption of "The New Consumer Agenda" in 2020, which had defined long-term objectives in the field of consumer protection, including the green transition, digital transformation, redress and enforcement of consumer rights, the specific needs of certain consumer groups, and international cooperation.⁹⁵ The new Consumer Agenda 2030 highlights that consumers within the EU enjoy one of the strongest levels of protection in the world, yet they continue to face numerous challenges, such as high living costs and socio-economic insecurity, climate change, exposure to unsafe products and unfair commercial practices (particularly online), barriers to cross-border shopping, and difficulties in obtaining redress.⁹⁶ It defines four priority areas for development: an action plan for consumers in the Single Market, digital fairness and online consumer protection, sustainable consumption, and enforcement and redress.⁹⁷

⁹³ Consolidated version of the Treaty on the Functioning of the European Union, Official EN Journal of the European Union C 326/47, 26.10.2012., Art. 4 (2), Art. 12., Art. 114 (3) and Art. 169.

⁹⁴ European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Consumer Agenda and action plan for consumers in the single market 'A new impulse for consumer protection, competitiveness and sustainable growth', Brussels, 19.11.2025., https://commission.europa.eu/strategy-and-policy/policies/consumers/consumer-protection-policy/2030-consumer-agenda_en, 18 February 2026. (hereinafter referred to as: Consumer Agenda 2030)

⁹⁵ See: Legislative Train 12.2025: 3. Supporting People, Strengthening Our Societies and Our Social Model, <https://www.europarl.europa.eu/legislative-train/carriage/e-declaration-portal-for-posting-workers-in-the-eu/report?sid=9801>, 18 February 2026.

⁹⁶ See: Consumer Agenda 2030, p. 1.

⁹⁷ For a detailed discussion of the aforementioned areas and the planned measures for their development, see *Ibid.*, pp. 2 *et seq.*

3.2.1. Directive (EU) 2023/2673

The Consumer Agenda 2030 has identified cross-border provision of financial services as one of the areas where consumers face obstacles. Although the share of consumers purchasing financial services abroad has increased, in certain categories this number remains very limited, particularly in relation to consumer credit, mortgage loans, and insurance. Accordingly, cooperation between the European Commission and Member States is envisaged to ensure effective implementation and enforcement of existing financial services directives.⁹⁸ One such directive is Directive (EU) 2023/2673. This directive represents a significant update to the EU legislation on distance contracts for financial services. Adopted in the context of accelerated digitalisation of the financial sector and the emergence of new financial services, its aim is to provide enhanced consumer protection while maintaining an environment conducive to innovation. The primary motivation is to adapt to digital realities, characterised by the exponential growth of online contracts and the emergence of innovative financial products, such as those linked to crowdfunding and cryptocurrencies. The aim of the Directive (EU) 2023/2673 is to balance technological innovation with the need to protect consumers from manipulative practices.⁹⁹

3.2.2. Directive (EU) 2024/825

Directive (EU) 2024/825, also known as the "Directive on Empowering Consumers," aims to further protect consumer rights within the EU by supplementing the existing EU list of prohibited commercial practices. It is based on the premise that, in order for consumers to contribute effectively to the green transition toward a circular economy, they must not be misled by unfair commercial practices that prevent them from making sustainable acquisitions. Under Directive (EU) 2024/825, new rules have been introduced to prevent the negative impact of unfair commercial practices, such as premature and planned obsolescence of products, greenwashing, and misleading claims regarding social, environmental, or circular features of products, including aspects such as longevity, reparability, or reusability.¹⁰⁰ The Directive amends Directive

⁹⁸ See: *Ibid.*, p. 4.

⁹⁹ See: Sandu, F., *Innovation vs. Protection: How to Balance Directive (EU) No. 2023/2673 Online Financial Services Market?*, Pandectele Romane, no. 1/2025, p. 115.

¹⁰⁰ Proso, M., *Planned Obsolescence of Products as a Form of Unfair Commercial Practice and the Right to Repair – New Means of Protecting Consumer Rights in the European Union*, SEE Law Journal, no. 13/2024, p. 33.

2005/29/EC¹⁰¹ concerning rules on early obsolescence practices, including planned obsolescence, which is defined as a business policy involving the deliberate planning or design of a product with a limited lifespan so that it becomes prematurely obsolete or non-functional after a certain period or after a predetermined level of use.¹⁰² Additionally, Directive (EU) 2024/825 introduces amendments to Directive 2011/83/EU of the European Parliament and of the Council on consumer rights¹⁰³, primarily imposing obligations on traders to provide clear, relevant, and reliable information regarding the existence of commercial guarantees, the reparability of goods, statutory conformity, warranties, and other related consumer rights.¹⁰⁴

3.2.3. Directive (EU) 2024/1799

Directive (EU) 2024/1799, also known as the "Right to Repair Directive," was adopted on 13 June 2024. It introduces rules aimed at enhancing the reparability of goods and amends Regulation (EU) 2017/2394¹⁰⁵, Directive (EU) 2019/771, and Directive (EU) 2020/1828¹⁰⁶. The new provisions of this Directive are designed to reduce waste by enabling longer use of various products through regulation of the right to repair, both during and after the warranty period.¹⁰⁷

¹⁰¹ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), Official Journal of the European Union, L 149, 11 June 2005 (hereinafter referred to as: Directive 2005/29/EC)

¹⁰² Directive (EU) 2024/825, Recital 16, in comparison with Directive 2005/29/EC, Chapter 2.

¹⁰³ Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance, Official Journal of the European Union, L 304, 22 November 2011 (hereinafter referred to as: Directive 2011/83/EU)

¹⁰⁴ See: Directive (EU) 2024/825, Art. 2.

¹⁰⁵ Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004, Official Journal of the European Union, L 345, 27 December 2017

¹⁰⁶ Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, Official Journal of the European Union, L 409, 4 December 2020

¹⁰⁷ Proso, M., *op. cit.* in fn. 100, p. 33.

Repairing products is generally more effective than recycling and can serve as an important means to reduce waste and extend the lifespan of goods, which is widely recognised as one of the objectives of the circular economy.¹⁰⁸ However, consumers do not always choose to repair a defective product rather than replace it, for a variety of reasons. These include the cost of repair relative to the cost of replacement, associated repair expenses such as travel costs and waiting time, so-called product obsolescence due to the arrival of new models on the market, and the consumer's perception of repair quality.¹⁰⁹ In the past, it was common for consumers to perform simple repairs themselves or to hire independent repairers for more complex faults. This practice has largely disappeared today because modern technical goods operate with embedded electronics, which require specialised knowledge for repair. Additionally, electronic products evolve much faster than other types of goods, becoming obsolete in a shorter period, while new and improved models enter the market. Electronic components in such products also fail more quickly than other parts, necessitating more frequent repairs.¹¹⁰ Moreover, manufacturers of technical goods further limit consumers' ability to repair products by incorporating software over which they hold intellectual property rights. Legally, this means that repairs on such software can only be performed by the manufacturer or an authorised service provider, not by independent repairers.¹¹¹ There are also beliefs that the shorter lifespan of electronic products is not accidental, but the result of deliberate actions by manufacturers, who incorporate components with planned obsolescence.¹¹² Directive (EU) 2024/1799 promotes sustainable consumption and environmental protection by encouraging longer product lifespans, including reuse, repair, and refurbishment. At the same time, the benefit to consumers lies in reducing consumption through a decreased need to purchase new products.¹¹³ This Directive is one of maximum harmonisation, as Article 3 stipulates that Member States may neither retain nor introduce provisions in their national law that deviate from the Directive's requirements.¹¹⁴

¹⁰⁸ See: Terryn, E., *A Right to Repair? Towards Sustainable Remedies in Consumer Law*, European Review of Private Law, vol. 27, no. 4/2019, p. 853.

¹⁰⁹ See in detail in: McCollough, J., *Consumer Discount Rates and the Decision to Repair or Replace a Durable Product: A Sustainable Consumption Issue*, Journal of Economic Issues, vol. 44., no. 1/2010., pp. 183–204.

¹¹⁰ Jovičić, K., *The EU Right-to-Repair Directive: Why Do We Need Legal Protection of This Right via Imperative Legal Norms?*, Review of European Law, vol. 26., no. 1/2024, p. 105.

¹¹¹ Proso, M., *op. cit.* in fn. 100, p. 38.

¹¹² Buseman, N. A., *A Second Generation Solution to Electronic Waste: The New York Approach*, Columbia Journal of Environmental Law, vol. 37, no. 2/2012, pp. 145–146.

¹¹³ Proso, M., *op. cit.* in fn. 100, p. 39.

¹¹⁴ See: Directive (EU) 2024/1799, Art. 3.

4. MAIN FEATURES AND INNOVATIONS IN THE DRAFT AMENDMENTS TO THE CONSUMER PROTECTION ACT¹¹⁵

4.1. Reasons for Adoption and Key Innovations in the Draft Proposal

As previously noted, the primary reasons for adopting the Draft Proposal are the transposition of Directive (EU) 2023/2673, Directive (EU) 2024/825, and Directive (EU) 2024/1799, as well as the need for clearer regulation of existing and the introduction of new trader obligations, and ensuring a high level of consumer protection through more precise rules on specific forms of product sales and stricter sanctions for violations. Although the current CPA prescribes a wide range of obligations regarding pre-contractual information¹¹⁶, including the mandatory provision of all relevant details on the terms and consequences of contract conclusion, practice has shown that, due to the large volume of information, consumers often do not receive clearly highlighted key data that are crucial for making purchasing decisions. The new Draft Proposal seeks to address this shortcoming by specifically regulating pre-contractual information in the context of distance contracts for financial services. Special attention is also given to the provision of information on the environmental and social characteristics of products, as well as to general aspects of the trader's business. Furthermore, the Draft Proposal foresees the introduction of new labels informing consumers about liability for material defects and commercial guarantees regarding product durability, with the option to use the European standardised form for repair information.¹¹⁷

4.1.1. Pre-Contractual Consumer Information and Regulation of Misleading Commercial Practices Related to Environmental and Social Claims

The expansion of trader obligations regarding pre-contractual consumer information is a result of the transposition of Directive (EU) 2024/825, and primarily concerns the duty to provide consumers with more detailed information on liability for material defects and commercial guarantees. Although traders are

¹¹⁵ The Draft Proposal for the Amendments to the Consumer Protection Act, published on the e-consultation portal of the Government of the Republic of Croatia (<https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=32306>, 19 February 2026) and hereinafter is referred to as the Draft Proposal.

¹¹⁶ See: CPA, Art. 46., Art. 60., Art. 88.

¹¹⁷ See: *supra*, p. 1.-2. and the Draft Proposal

already required to inform consumers about these legal instruments¹¹⁸, practice has shown that such information is often not adequately communicated. Until now, the manner of fulfilling this obligation has been left to the discretion of the trader, who decided on the most appropriate form and method of providing the information. In response to this issue, the Draft Proposal foresees the introduction of specific labels that clearly highlight both legal instruments and their characteristics, through the addition of new points in Articles 46 para. 1. and Art. 60. para. 1 of the CPA. These provisions separately and in detail establish traders' obligations to inform consumers regarding liability for material defects, liability for the conformity of digital content or digital services, commercial guarantees, free commercial durability guarantees for periods exceeding two years, the minimum period during which the manufacturer or supplier of digital content or services provides updates for goods with digital elements, and the assessment of product reparability.¹¹⁹ These labels are harmonised at the EU level and regulated by Commission Implementing Regulation (EU) 2025/1960 of 25 September 2025 on the design and content of the harmonised notice on the legal guarantee of conformity and of the harmonised label for the commercial guarantee of durability¹²⁰. In Croatian legislation, the content of this Regulation will be further detailed in a by-law to be adopted by the minister competent for consumer affairs. As liability for material defects rests exclusively with the trader–seller, they will be obliged to display notices regarding material defects at their points of sale (in stores, on online shop websites, etc.) in a clearly visible manner. Conversely, labels indicating the duration of a given commercial durability guarantee will generally be displayed directly on the product itself.¹²¹ The provisions of the Draft Proposal resulting from the transposition of Directive (EU) 2024/825 also regulate misleading commercial practices related to environmental and social claims. Although such practices can be assessed under the general provisions of the CPA prohibiting misleading commercial practices¹²², they may be the subject to varying interpretations. To address this, the Draft Proposal supplements the “blacklist” of misleading commercial practices and establishes targeted provisions concerning misleading claims about early product obsolescence¹²³, claims regarding

¹¹⁸ CPA, Art. 46. para. 1. and Art. 60. para. 1.

¹¹⁹ See Draft Proposal, Art. 20. para. 1. Article 23 of the Draft Proposal envisages the insertion of identical provisions into Art. 60 of the CPA, which regulates the provision of pre-contractual information in the context of off-premises and distance contracts.

¹²⁰ Official Journal of the European Union L 2025/1960, 2.10.2025.

¹²¹ See: Draft Proposal.

¹²² See: CPA, Art. 35. – 37.

¹²³ Draft Proposal, Art. 17.

environmental friendliness ("manipulative green marketing")¹²⁴, and non-transparent or unreliable sustainability labels¹²⁵.

4.1.2. Amendments Related to Unilateral Termination of Contracts Concluded via Online Interfaces and Distance Contracts for the Sale of Financial Services

The provisions of the Draft Proposal regulating distance sales of financial services are largely the result of transposing Directive (EU) 2023/2673. Based on the premise that financial services are often complex for consumers and that understanding the associated risks is frequently insufficient, the Draft Proposal explicitly establishes the consumer's right to additional clarification of the proposed contractual terms. Specifically, the previous provision of Article 88 of the CPA, which required that the consumer be informed within a reasonable period prior to concluding the contract about the trader, the financial service concerned, the contract details, and the dispute resolution procedure—while generally referring to information provided elsewhere in that part of the Act¹²⁶—has been replaced by a new provision in the same article. In paragraph 1, 25 points now precisely list the pre-contractual information that the trader must provide to the consumer within a reasonable period before concluding the contract or before making a binding offer. Furthermore, paragraphs 2–11 of Article 88 regulate in detail the manner in which the prescribed information must be delivered.¹²⁷ In addition, Article 90 of the Act has been renamed "Clarification of Contractual Terms" and explicitly establishes the consumer's right to request further explanation of the proposed contractual provisions.¹²⁸ Such clarifications must not be limited to a formal repetition of already provided pre-contractual information; rather, they must elaborate on the key elements of the contract—particularly the retail price, the duration of the contractual relationship, and other essential terms—so that the consumer can assess the alignment of the contractual content and associated services with their needs and financial capacity. It should be noted that Directive (EU) 2023/2673 is, by its legal nature, a directive of maximum harmonisation, which leaves very limited scope for additional regulatory intervention. Nevertheless, the Draft Proposal goes further in the context of pre-contractual information regarding distance contracts for the sale of financial services by requiring the trader to provide information on the risk–return profile

¹²⁴ See: *Loc. cit.*

¹²⁵ See: *Loc. cit.*

¹²⁶ See: CPA, Art. 88.

¹²⁷ See: Draft Proposal, Art. 31.

¹²⁸ *Loc. cit.*

of the transaction. This represents an optional regulatory measure available to Member States, which Croatia supported during the negotiations on the adoption of the Directive. Accordingly, the Draft Proposal establishes an obligation to inform consumers of all risks relevant to the specific financial service offered, including the precise indication of the maximum potential capital loss and explicit information on the possibility of total loss of invested funds.¹²⁹ Given that such information can have a decisive impact on the consumer's decision to enter into a distance contract for financial services, the Croatian legislator has decided to make it a mandatory element of pre-contractual information. One of the most significant innovations arising from the transposition of this Directive, applicable to all distance contracts, is the introduction of a functionality for unilateral termination of a distance contract—commonly referred to as the “unilateral termination button.”¹³⁰ This is a technical solution that traders will be required to implement on their websites to allow consumers to terminate the contract as easily as it was concluded.¹³¹ The aim of this measure is to ensure that the process of terminating a contract concluded via an online interface is as simple and accessible as the act of entering into the contract itself.¹³² While implementing such functionality will require additional technical and financial investment by traders in their information systems and websites, this regulatory solution contributes to strengthening consumer protection and enables the effective exercise of the right to unilateral termination of distance contracts in its full scope.¹³³

4.1.3. Amendments Regulating the Repair of Goods in Relation to the Right to Repair Directive

The Draft Proposal contains provisions aimed at strengthening consumers' right to repair products, resulting from the transposition of Directive (EU) 2024/1799. These regulatory interventions focus on extending the lifespan of products and reducing waste, while simultaneously enhancing consumer awareness and legal certainty in exercising the right to repair. Accordingly, the Draft Proposal introduces a new Chapter IV.a into the CPA, entitled “Repair of Goods,” which is

¹²⁹ *Loc. cit.*

¹³⁰ Draft Proposal, Art. 27.

¹³¹ Pursuant to the current Art. 81 of the CPA, the consumer exercised the right to unilaterally terminate the contract by notifying the trader of their intention to withdraw, either through a standard contract withdrawal form or any other clear and unambiguous declaration expressing the consumer's will to terminate the contract, delivered by post or electronically.

¹³² Draft Proposal, Art. 42.

¹³³ See: Draft Proposal.

divided into four sections.¹³⁴ Section 1, titled "General Provisions," contains definitions of key concepts within the scope of this Chapter. Section 2, titled "Information on the Right to Repair Goods," establishes the obligation of repairers to provide consumers with essential information regarding the terms and scope of repair services. This section also introduces the European Repair Information Form, which repairers may voluntarily use in their business operations.¹³⁵ This is a standardized document containing the essential elements of an offer to conclude a repair contract, such as the identity of the repairer and basic information about them, the goods which are subject to the service, the nature of the defect, the type of proposed repair service, the retail price of the repair, the expected repair time, and other relevant details.¹³⁶ Although repairers are already obliged under the current framework to provide most of this information as part of pre-contractual disclosure¹³⁷, the standardization of the form contributes to greater clarity and consistency in practice.¹³⁸ It facilitates compliance with legal obligations for repairers while presenting information to consumers in a clear, organized, and easily understandable manner tailored to their needs. Section 3 of the new Chapter IV.a, entitled "Obligations of the Manufacturer – Producer," introduces new duties for manufacturers – and, subsidiarily, importers, distributors, and authorized representatives¹³⁹ – regarding the repair of products in accordance with reparability requirements established by the relevant EU provisions.¹⁴⁰ Among the most significant innovations is the prohibition on refusing a repair solely because the product has previously been repaired by another party, including unauthorized repairers or the consumer themselves. This limits practices that traditionally led to unjustified denial of service and encouraged product replacement instead of repair. Furthermore, contractual or technical measures that hinder repair are prohibited, whether through restrictive contractual clauses or the use of hardware or software solutions that prevent or significantly impede intervention on the product. Additionally, the use of original, used, compatible, or 3D-printed spare parts by independent repairers cannot be prevented, provided such parts comply with EU and national law, including product safety requirements and intellectual property rights rules. This provision is particularly important for preserving market competition and ensuring the sustainability of independent repair business

¹³⁴ See: Draft Proposal, Art. 44.

¹³⁵ Draft Proposal, Art. 44.

¹³⁶ *Loc. cit.*

¹³⁷ See: CPA, Art. 69.

¹³⁸ Draft Proposal, Art. 44.

¹³⁹ See: Draft Proposal, Art. 4. (...) Section 3: Obligations of the producer – manufacturer (...) Art. 112.e, para. 6–8.

¹⁴⁰ See: Draft Proposal, Art. 44. (...) Section 3.: Obligations of the producer - manufacturer (...) Art. 112.e

activities.¹⁴¹ Finally, Section 4 of the new Chapter IV.a, titled "European Repair Platform," provides for the use of a national section of the shared European online repair platform, enabling consumers to locate repairers, sellers of refurbished goods, or local community initiatives promoting product repair that voluntarily register on the platform. Access to the national section of the European Repair Platform is free of charge for consumers.¹⁴²

4.1.4. Other Significant Innovations in the Draft Proposal

In addition to the amendments resulting from the alignment with the aforementioned EU Directives, the Draft Proposal introduces several other significant innovations aimed at strengthening the position of consumers. In particular, it provides clearer regulation regarding the determination and display of prices during special forms of sales¹⁴³, i.e., during various types of discounts. Specifically, the provision of the current Article 19, paragraph 2 of the CPA, which requires that during the duration of a special sale the trader must display, alongside the discounted price, the lowest price applied for the same product during the 30-day period preceding the special sale, has caused practical uncertainties concerning whether it also requires determining the level of the discounted price in relation to the lowest price previously applied by the trader for the same product during the 30 days prior to the special sale. The Court of Justice of the European Union¹⁴⁴ addressed this issue in the case *Verbraucherzentrale Baden-Württemberg eV v Aldi Süd Dienstleistungs SE & Co. OHG*¹⁴⁵, confirming that the lowest price applied to a product during the 30-day period preceding the special sale constitutes the reference price for determining the discounted price.¹⁴⁶ In line with this ruling, the Draft Proposal amends Articles 19 and 20 of the CPA so that the reference point for determining the discounted price, instead of the regular sale price, is the price in accordance with the aforementioned position of the CJEU.¹⁴⁷ The amendment to Article 19 of the CPA, i.e., Article 9 of the Draft Proposal, provides

¹⁴¹ See: Draft Proposal, Art. 44. (...) Section 3.: Obligations of the producer - manufacturer (...) Art. 112.g

¹⁴² See: Draft Proposal, Art. 44. (...) Section 3.: Obligations of the producer - manufacturer (...) Art.112.h – 112.l

¹⁴³ In accordance with the provisions of Article 19, paragraphs 1 and 2 of the CPA, special forms of sale are considered to be the sale of products at prices lower than regular retail prices, which includes, among others, promotional sales, clearance sales, seasonal discounts, the sale of defective goods, and the sale of goods approaching their expiration date.

¹⁴⁴ Hereinafter referred to as: CJEU.

¹⁴⁵ Judgement of 26. 9. 2024. – Case C-330/23

¹⁴⁶ See: *Loc. cit.*

¹⁴⁷ See: Draft Proposal, Art. 9. – 10.

an exception to the aforementioned obligation for the sale of perishable goods and products close to their expiration date, whose prices are naturally reduced more frequently to facilitate quicker sales. In such cases, it is not reasonable to require that the discounted price be determined with reference to the lowest price over the preceding 30 days.¹⁴⁸ Furthermore, the Draft Proposal, through the amendment of Article 21 of the CPA, introduces the possibility of progressive price reductions during clearance sales¹⁴⁹, which was previously not permitted. Until now, any further price reduction during a clearance sale required the initiation of a new special sale. This amendment enables consumers to purchase goods at more favorable prices while allowing traders to more easily sell remaining stock.¹⁵⁰ A welcome amendment that strengthens consumers' right to protection from harassment is the provision of Article 8 of the Draft Proposal, which supplements Article 18 of the CPA regarding the delivery of advertising messages and materials. The amendment explicitly prohibits the sending of advertising messages and materials to a consumer who has clearly and unequivocally expressed to the trader their objection, including cases where advertising messages or materials are delivered together with the invoice for the purchased product.¹⁵¹ The Draft Proposal also introduces certain changes concerning the supervision and enforcement of consumer rights. Specifically, in the areas of hospitality services, tourism services, and accommodation fees, exclusive authority is granted to the Tourism Inspectorate of the State Inspectorate, encompassing inspection tasks related to monitoring unfair practices by traders providing hospitality and tourism services.¹⁵² For the purposes of this research, it is of particular interest that the Draft Proposal increases the maximum regulatory fines that may be imposed on traders for violations of the provisions of the CPA, as it has been shown that the currently applicable fine framework does not provide a sufficient deterrence.¹⁵³ Thus, the previously prescribed maximum fine for a misdemeanour under Article 149 of the CPA, which amounted to HRK 200,000.00, has been replaced by an amount of EUR 50,000.00, representing an increase of approximately 88.5%. The Draft Proposal also adjusts the amounts of fines for offenses causing harm to collective consumer interests and rights, offenses committed by responsible persons in legal entities with public authority or local government units, as well as offenses by traders operating electronic communications services, which were

¹⁴⁸ *Loc. cit.*

¹⁴⁹ It should be noted that the reference price for determining the discounted price remains the lowest price at which the goods were offered during the 30-day period preceding the commencement of the special form of sale.

¹⁵⁰ See: Draft Proposal, Art. 11.

¹⁵¹ See: Draft Proposal, Art. 8. in comparison to CPA, Art. 18.

¹⁵² See: Draft Proposal, Art. 46.

¹⁵³ This issue has been highlighted through a review of the relevant case law in the application of the CPA. See *supra*, p. 9 sq.

previously expressed in Croatian kuna and now need to be presented in euros.¹⁵⁴ Finally, the Draft Proposal foresees the adoption of implementing regulations to define the content of the harmonized notice and label containing information on the minimum duration of liability for material defects and commercial guarantees, as well as a regulation establishing the content of the European repair information form.¹⁵⁵ The Draft Proposal provides for an eight-day *vacatio legis*, except for provisions transposing Directive (EU) 2023/2673, Directive (EU) 2024/825, and Directive (EU) 2024/1799, which are set to enter into force on 27 September 2026.

¹⁵⁶

4.2. Implications for the Position of Consumers, Proposals, and Final Results of the e-Consultation

As previously noted, during the drafting of the Draft Proposal, it was assumed that due to the large volume of information that must be provided to consumers, the notifications crucial for purchasing decisions are often insufficiently highlighted, meaning that consumers may ultimately be deprived of the most important information about their rights. The proposed innovations in the CPA concerning pre-contractual information, the introduction of standardized labels informing consumers about the content of rights related to liability for material defects and commercial guarantees, as well as clearer regulation of provisions regarding price display during special forms of sales, ensure a higher level of consumer awareness about their rights, thereby increasing the likelihood of these rights being effectively exercised in practice. The strengthening of consumers' position and rights is also promoted through facilitating product repair; by regulating manufacturers' obligations to repair goods, prohibiting refusal of repair on the grounds that the product was previously repaired by others, and introducing the European Repair Platform and the European Repair Information Form. By making repairs more accessible to consumers, the need to purchase new goods is reduced, which can ultimately lead to the production of higher-quality, longer-lasting products, especially considering the prohibition of false claims regarding planned obsolescence. Deterrence of traders from unfair commercial practices is also intended to be achieved by increasing the maximum amounts of regulatory fines for violations of the CPA. It should nevertheless be noted that the Draft Proposal, as a deterrent measure against the commission of offences, provides for an increase

¹⁵⁴ See: Draft Proposal, Art. 54. – 57. The conversion of monetary penalties from kuna to euros has, by its very nature and due to rounding, resulted in minor adjustments to all total amounts compared to the previously prescribed figures.

¹⁵⁵ See: Draft Proposal, Art. 58.

¹⁵⁶ See: Draft Proposal, Art. 60.

only of the upper limit of fines, while the lower limit remains unchanged at EUR 1,500.00 (currently HRK 10,000.00). Furthermore, the fines for responsible persons within legal entities remain set within the range of EUR 1,500.00 to EUR 2,500.00 (currently HRK 10,000.00 to HRK 15,000.00), as is also the case for traders who are natural persons, for whom fines are prescribed in the range of EUR 750.00 to EUR 2,500.00 (currently HRK 5,000.00 to HRK 15,000.00). Although the legislator has evidently recognised the issue of the insufficient deterrent effect of the prescribed sanctions for breaches of the CPA, it appears that the problem has been inadequately addressed, and that the amendments introduced by the CPA in this regard will neither increase the deterrent effect of misdemeanour sanctions nor contribute to a reduction in the number of infringements. A review of the case law of misdemeanour courts clearly shows that courts impose fines for CPA-related offences at very low levels, often at the very lower limit of the prescribed range, frequently also applying the institute of mitigation of penalties.¹⁵⁷ Therefore, increasing the maximum amount of administrative fines will, in practice, have no meaningful effect, as misdemeanour courts predominantly impose penalties at the lower rather than the upper end of the statutory range. Potential offenders are therefore likely to rely, notwithstanding any theoretical deterrent effect of higher maximum penalties, on established case law indicating that sanctions for such infringements are lenient and that the gains achievable through non-compliance outweigh the potential losses.¹⁵⁸ It therefore appears that a significantly stronger deterrent effect would be achieved by increasing the lower, rather than the upper, limit of misdemeanour fines. This would almost certainly lead to higher fines being imposed in practice in proceedings concerning violations of the CPA, as courts would be obliged to operate within a higher statutory range. Even in cases where the institute of penalty mitigation is applied, the final sanctions would still be higher than those currently imposed. Potential offenders would thus be able to rely with greater certainty on the likelihood of stricter punishment. The solution proposed in the Draft Proposal does not lead to a real, practical increase in fines, as it merely grants courts the possibility of imposing higher penalties, which they may, but are not obliged to, apply. Given the review of existing case law, it is likely that courts will not make use of this possibility to any significant extent. The public e-consultation on the Draft Amendment, which ran until 21 January 2026, generated significant interest from the public, traders, and consumer protection associations, resulting in a total of 104 comments on the draft text.¹⁵⁹ Consumer protection associations, as well as individual consumers,

¹⁵⁷ See: *supra*, p. 9 sq.

¹⁵⁸ This is evidenced by the large number of cases concerning the use of unfair commercial practices, as well as by the fact that there are 'repeat offenders' among the perpetrators. See: *supra*, p. 11.

¹⁵⁹ See: Draft Proposal.

highlighted in their comments several challenges regarding consumer rights protection, including incorrect or incomplete information about guarantees, issues with the quality and conformity of goods in stores, placing food and cosmetic products on the market without prior safety verification, and obstacles to exercising rights in cases of material defects.¹⁶⁰ A request was also raised to establish a legal obligation for traders to provide consumers with a replacement device during the repair period when the item is needed for daily use, as one of the most frequent consumer complaints concerns prolonged repairs without any compensation. This request was rejected because the matter is already regulated under the COA, and Directive (EU) 2024/1799, by its nature as a directive of maximum harmonization, does not grant consumers the right to a replacement item during repair unless the manufacturer or seller provides one.¹⁶¹ Electronic communications operators opposed the introduction of the functionality for unilateral contract termination—commonly referred to as the “unilateral termination button”—arguing that this area is already regulated by specific provisions of the Croatian Regulatory Agency for Network Activities; these proposals were also rejected.¹⁶² Finally, consumer protection associations proposed that, regarding the introduction of the European Repair Information Form, the obligation for service providers to issue the form should be mandatory rather than optional. This proposal was also rejected because the provision reflects the implementation of Directive (EU) 2024/1799, from which deviations are not permitted.¹⁶³

5. CONCLUSION

The Draft Proposal for the Amendments to the Consumer Protection Act introduces a series of significant innovations aimed at strengthening consumer rights and enhancing legal certainty regarding consumer protection in Croatia. Among the most notable changes are the improved pre-contractual information obligations, the introduction of standardized labels informing consumers about liability for material defects and commercial warranties, the regulation of misleading environmental and social claims, and the clearer rules regarding the display of prices during special sales events. Furthermore, the Draft Proposal

¹⁶⁰ See: Draft Proposal, Comments, <https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=32306>, 23 February 2026

¹⁶¹ See: Draft Proposal, Art. 6., Comments, <https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=32306>, 23 February 2026

¹⁶² See: Draft Proposal, Art. 27., Comments, <https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=32306>, 23 February 2026

¹⁶³ See: Draft Proposal, Art. 44., Comments, <https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=32306>, 23 February 2026

implements provisions arising from EU Directives (EU) 2023/2673, (EU) 2024/825, and (EU) 2024/1799, including the regulation of distance contracts for financial services, the facilitation of unilateral contract termination online, and the reinforcement of the right to repair, including the establishment of a European Repair Platform and the European Repair Information Form. These legislative innovations have profound implications for consumer protection. By increasing transparency and clarity in pre-contractual communication, consumers are better informed about their rights and can make more deliberate purchasing decisions. The emphasis on the right to repair and the regulation of misleading product claims promotes sustainable consumption, reduces unnecessary waste, and encourages producers to design longer-lasting and more reliable products. Although the aforementioned legislative innovations have significant implications for consumer protection, it is our view that the Draft Proposal missed an opportunity to address what may be the most significant problem of consumer protection law in the Republic of Croatia—namely, its enforcement in practice. The legislative framework of consumer protection law in Croatia has been considerably improved and is largely well aligned with relevant EU legislation; however, a review of the (insufficient) case law clearly shows that consumers do not make use of the available mechanisms for protecting their rights and that the provisions of the CPA continue to be infringed in practice. Despite the recognition that the current framework of prescribed misdemeanour fines for breaches of the CPA lacks a sufficient deterrent effect, this issue has not been addressed in light of judicial practice, and the established tendency of misdemeanour courts to impose very low fines under Article 149 of the CPA appears to have been overlooked. The increase of maximum fines from HRK 200,000.00 to EUR 50,000.00—i.e. by almost 90%—appears largely ineffective in a context where misdemeanour courts rarely impose fines exceeding EUR 3,000.00 on legal persons, i.e. traders. It seems that, from a *de lege ferenda* perspective, increasing the minimum level of fines would have a far more effective deterrent effect, as it would compel courts to impose more substantial sanctions, thereby contributing to the effective enforcement of consumer protection rules, as opposed to their merely nominal existence without practical application. Furthermore, from a *de lege ferenda* perspective, further improvements could include mandatory issuance of the European Repair Information Form by service providers to ensure consistent consumer access to repair information, the introduction of minimum standards for compensation or replacement during lengthy repairs, and continued monitoring of digital platforms to safeguard consumer rights in online and cross-border transactions. Such measures would further consolidate the position of consumers as informed, empowered, and active participants in a dynamic and sustainable market environment.

REFERENCES

BOOKS AND ARTICLES

1. Babić, M., *Zaštita prava potrošača i izvori trgovačkog prava*, Poslovna izvrsnost, vol. IX, No. 1/2015., pp. 71–90.
2. Baretić, M., *Individualna i kolektivna zaštita potrošača u hrvatskom pravu*, in: Tomljenović, V.; Čulinović Herc, E.; Butorac Malnar, V. (eds.), *Republika Hrvatska na putu prema Europskom pravosudnom području – rješavanje trgovačkih i potrošačkih sporova*, Pravni fakultet Sveučilišta u Rijeci, Rijeka 2009., pp. 241–286.
3. Baretić, M., *Zaštita potrošača u Republici Hrvatskoj nakon ulaska u Europsku uniju: jesmo li implementacijom europskog prava izgradili sustav zaštite potrošača?*, in: Bourgoignie, T.; Jovanović, T. (eds.), *Strengthening Consumer Protection in Serbia: Liber Amicorum Svetislav Taboroši*, Pravni fakultet Univerziteta u Beogradu, Beograd 2013., pp. 65–112.
4. Buseman, N. A., *A Second Generation Solution to Electronic Waste: The New York Approach*, Columbia Journal of Environmental Law, vol. 37, no. 2/2012, pp. 101–146.
5. Čikara, E., *Hrvatska – zakonodavne tehnike*, in: Jessel-Holst, C.; Galev, G. (eds.), *EU Consumer Contract Law; Potrošačko ugovorno pravo Evropske unije*, Civil Law Forum for South East Europe Collection of Studies and Analyses, vol. III, Beograd-Zagreb 2010., pp. 592–595.
6. Dabović Anastasovska, J., *Implementacija novina potrošačkog prava Europske unije u potrošačke zakone zemalja regije*, Zbornik radova građanskog i trgovačkog zakonodavstva i pravne prakse, no. 20., Mostar 2023., pp. 7–35.
7. Jokanović, I.; Dudás, A., *Lack of Conformity and Seller's Liability in Croatian, Slovenian and Serbian Law*, Zbornik Pravnog fakulteta u Zagrebu, vol. 75, no. 4/2025, pp. 551–585.
8. Josipović, T., *Das Konsumentenschutzgesetz – Beginn der Europäisierung des kroatischen Vertragsrechts*, in: Grundmann, S.; Schauer, M. (eds.), *The Architecture of European Codes and Contract Law*, Kluwer Law International, Vienna 2006., pp. 129–151.
9. Jovičić, K., *The EU Right-to-Repair Directive: Why Do We Need Legal Protection of This Right via Imperative Legal Norms?*, Review of European Law, vol. 26., no. 1/2024, pp. 97–115.
10. Kanceljak, I., *Reform of Consumer Sales Law of Goods and Associated Guarantees – Possible Impact on Croatian Private Law*, EU and Comparative Law Issues and Challenges Series (ECLIC), vol. 2/2018: EU Law in Context – Adjustment to Membership and Challenges of the

- Enlargement, University Josip Juraj Strossmayer of Osijek, Faculty of law Osijek, pp. 586–610.
11. Ledić, D., *Consumer Protection Law – A Separate Branch of the New Croatian Legal System*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 13., no. 1/1992., pp. 145–169.
 12. Maganić, A., *Predstavničke tužbe za zaštitu kolektivnih interesa i prava potrošača u Republici Hrvatskoj*, Zbornik radova „Aktualnosti građanskog i trgovačkog zakonodavstva i pravne prakse“, no. 20., Mostar, 2023., pp. 146–161.
 13. McCollough, J., *Consumer Discount Rates and the Decision to Repair or Replace a Durable Product: A Sustainable Consumption Issue*, Journal of Economic Issues, vol. 44., no. 1/2010., pp. 183–204.
 14. Mišćenić, E., *Croatian Case "Franak": Effective or "Defective" Protection of Consumer Rights?*, Harmonius: Journal of Legal and Social Studies in South East Europe, 2016., pp. 184–209.
 15. Mišćenić, E., *Europsko privatno pravo*, opći dio, Školska knjiga, Zagreb 2019.
 16. Mišćenić, E., *Sustainability, the Circular Economy and Consumer Law in Croatia*, Journal of European Consumer and Market Law, vol. 9., no. 4/2020, pp. 173–176.
 17. Mišćenić, E., *Usklađivanje prava zaštite potrošača u Republici Hrvatskoj*, Godišnjak Akademije pravnih znanosti Hrvatske, vol. IV, no. 1/2013., pp. 145–176.
 18. Petrašević, T.; Poretti, P., *Consumer Protection in Croatia with a Special Emphasis on Distance and off-Premises Contracts*, Journal for Legal Theory and Practice, Vol. 3., No. 1/2016., pp. 9–54.
 19. Poretti, P., *Sudska zaštita prava potrošača – (naj)bolji put?*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39., no. 1/2018, pp. 535–573.
 20. Pošćić, A., *Europsko pravo tržišnog natjecanja i interesi potrošača*, Narodne novine, Zagreb 2014.
 21. Proso, M., *Planned Obsolescence of Products as a Form of Unfair Commercial Practice and the Right to Repair – New Means of Protecting Consumer Rights in the European Union*, SEE Law Journal, no. 13/2024, pp. 32–41.
 22. Proso, M.; Milan Ostojić, F., *Zaštita (kolektivnih) interesa i prava potrošača i alternativno rješavanje potrošačkih sporova*, Zbornik radova IX. međunarodnog savjetovanja „Aktualnosti građanskog procesnog prava – nacionalna i usporedna pravnoteorijska i praktična dostignuća“, Split, 2023., pp. 173–196.

23. Salač, J.; Uzelac, J., *Zaštita potrošača u Republici Hrvatskoj u kontekstu harmonizacije s pravnom stečevinom Europske unije*, FIP - Financije i pravo, vol. 2, No. 2/2014, pp. 7–27.
24. Sandu, F., *Innovation vs. Protection: How to Balance Directive (EU) No. 2023/2673 Online Financial Services Market?*, Pandectele Romane, no. 1/2025, pp. 114–124.
25. Sukačić, M., *European Consumer in Sales Contract – the Ancient Approach, De Lege Lata & De Lege Ferenda*, EU and Comparative Law Issues and Challenges Series (ECLIC), no. 8., 2024., pp. 865–888.
26. Tepeš, N., *Izvansudsko rješavanje potrošačkih sporova u Hrvatskoj*, in: Tomljenović, V.; Čulinović Herc, E.; Butorac Malnar, V. (eds.), *Republika Hrvatska na putu prema Europskom pravosudnom području: Rješavanje trgovačkih i potrošačkih sporova*, Pravni fakultet Sveučilišta u Rijeci, Rijeka 2009., pp. 171–200.
27. Terryn, E., *A Right to Repair? Towards Sustainable Remedies in Consumer Law*, European Review of Private Law, vol. 27, no. 4/2019, pp. 851–873.
28. Weatherhill, S., *EU Consumer Law and Policy*, Edward Elgar Publishing Ltd, Cheltenham; Northampton 2005.

LEGAL RULES

1. Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Croatia, of the other part, Official Gazette – International Treaties no. 14-132/0
2. Consumer Protection Act, Official Gazette No. 96/2003, 46/2007, 79/2007
3. Consumer Protection Act, Official Gazette No. 79/2007, 125/2007, 79/2009, 89/2009, 75/2009, 133/2009, 78/2012, 56/2013, 41/2014
4. Consumer Protection Act, Official Gazette No. 41/2014, 110/2015, 14/2019, 19/2022
5. Consumer Protection Act, Official Gazette No. 19/2022, 59/2023
6. General Customs for the Trade of Goods, Official Gazette of the FNRJ No. 15/1954, Official Gazette of the SFRY No. 29/1978, Official Gazette No. 53/1991, 35/2005
7. Fundamental Act on the Trade of Goods, Official Gazette of the SFRY No. 1/1967
8. Civil Obligations Act, Official Gazette of the SFRY No. 29/1978, 39/1985, 46/1985, 57/1989, Official Gazette No. 53/1991, 73/1991, 3/1994, 111/1993, 107/1995, 7/1996, 91/1996, 112/1999, 88/2001, 35/2005
9. Act on Adopting the Civil Obligations Act, Official Gazette No. 53/1991

10. Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, Official Journal of the European Communities, L 171, 07 July 1999
11. Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), Official Journal of the European Communities, L 210, 7 August 1985
12. Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, Official Journal of the European Union, L 136, 22 May 2019
13. Act on Certain Aspects of Contracts for the Supply of Digital Content and Digital Services, Official Gazette No. 110/2021.
14. Act on Unfair Advertising, Official Gazette No. 43/2009.
15. Act on Representative Actions for the Protection of the Collective Interests and Consumer Rights, Official Gazette No. 59/2023.
16. Act on Alternative Dispute Resolution in Consumer Matters, Official Gazette, No. 121/2016, 32/2019.
17. Council Resolution of 14 April 1975 on a preliminary programme of the European Economic Community for a consumer protection and information policy, Official Journal of the European Communities, C 92, 25 April 1975
18. Treaty on European Union, Official Journal of the European Communities, C 191, 29 July 1992
19. Charter of Fundamental Rights of the European Union, Official Journal of the European Communities C 364/1, 18.12.2000
20. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, Official Journal of the European Union, C 306, 17 December 2007
21. Consolidated version of the Treaty on the Functioning of the European Union, Official EN Journal of the European Union C 326/47, 26.10.2012.
22. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), Official Journal of the European Union, L 149, 11 June 2005
23. Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities

- responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004, Official Journal of the European Union, L 345, 27 December 2017
24. Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, Official Journal of the European Union, L 409, 4 December 2020
 25. Commission Implementing Regulation (EU) 2025/1960 of 25 September 2025 on the design and content of the harmonised notice on the legal guarantee of conformity and of the harmonised label for the commercial guarantee of durability, Official Journal of the European Union L 2025/1960, 2.10.2025.
 26. Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC, Official Journal of the European Union L 2023/2673, 28.11.2023
 27. Directive (EU) 2024/825 of the European Parliament and of the Council of 28 February 2024 amending Directives 2005/29/EC and 2011/83/EU as regards empowering consumers for the green transition through enhanced protection against unfair commercial practices and improved information requirements, Official Journal of the European Union L 2024/825, 6.3.2024
 28. Directive (EU) 2024/1799 of the European Parliament and of the Council of 13 June 2024 on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394 and Directives (EU) 2019/771 and (EU) 2020/1828, Official Journal of the European Union L 2024/1799, 10.7.2024.
 29. Civil Procedure Act, Official Gazette of the SFRY No. 4/1977, 36/1977, 36/1980, 6/1980, 69/1982, 43/1982, 58/1984, 74/1987, 57/1989, 20/1990, 27/1990, 35/1991, and Official Gazette of the Republic of Croatia No. 53/1991, 91/1992, 112/1999, 129/2000, 88/2001, 117/2003, 88/2005, 2/2007, 96/2008, 84/2008, 123/2008, 57/2011, 25/2013, 89/2014, 70/2019, 80/2022, 114/2022, 155/2023, 146/2025."

COURT PRACTICE

1. Verbraucherzentrale Baden-Württemberg eV v Aldi Süd Dienstleistungs SE & Co. OHG, Judgement of 26. 9. 2024. – Case C-330/23
2. Supreme Court of the Republic of Croatia, case no. Revt-575/2016-5 of 3 October 2017.

3. High Misdemeanour Court of the Republic of Croatia case no. Ppž-7929/2024-2 of 20 February 2025,
4. High Misdemeanour Court of the Republic of Croatia case no. Ppž-2213/2025-2 of 26 November 2025,
5. High Misdemeanour Court of the Republic of Croatia case no. Gž-1263/2019-2 of 29 September 2021,
6. High Misdemeanour Court of the Republic of Croatia case no. Gž-129/2019 of 2 November 2021,
7. High Misdemeanour Court of the Republic of Croatia case no. Gž-50/2019 of 6 March 2019,
8. High Misdemeanour Court of the Republic of Croatia case no. Gž-1064/2018 of 10 April 2019,
9. High Misdemeanour Court of the Republic of Croatia case no. Ppž-6262/2025-2 of 15 July 2025,
10. High Misdemeanour Court of the Republic of Croatia case no. Ppž-13024/2022-2 of 15 July 2025,
11. Municipal Court in Novi Zagreb case no. Pp-81/2023-24 of 22 March 2024.
12. Constitutional Court of the Republic of Croatia case no. Usl-4002/13-11 of 3 June 2015.
13. Constitutional Court of the Republic of Croatia case no. Usl-3562/13-10 of 27 August 2015.,
14. Constitutional Court of the Republic of Croatia case no. Usl-1106/14-9 of 27 April 2016.
15. Constitutional Court of the Republic of Croatia case no. Usl-4304/13-8 of 9 September 2015.
16. High Misdemeanour Court of the Republic of Croatia case no. Gž-6360/10 of 24 April 2013,
17. High Misdemeanour Court of the Republic of Croatia case no. Gž-5044/11 of 16 April 2014
18. High Misdemeanour Court of the Republic of Croatia case no. Gž-5713/2011 of 24 October 2014.

NETWORK RESOURCES

1. National Consumer Protection Programme for the period 2005–2006. of 25 February 2005., https://www.hah.hr/pdf/program_zastite_potrosaca.pdf, 12 February 2026.
2. Ministry of Economy, National Consumer Protection Programme for the period until 2028, Zagreb, July 2025., <https://mingo.gov.hr/UserDocsImages/slike/Vijesti/2022/Nacionalni%20prog>

- ram%20za%C5%A1tite%20potro%C5%A1a%C4%8Da%20za%20razdoblje
 %20do%202028..pdf, 16 February 2026
3. Legislative Train 12.2025: 3. Supporting People, Strengthening Our Societies and Our Social Model, <https://www.europarl.europa.eu/legislative-train/carriage/e-declaration-portal-for-posting-workers-in-the-eu/report?sid=9801>, 18 February 2026.
 4. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Consumer Agenda and action plan for consumers in the single market 'A new impulse for consumer protection, competitiveness and sustainable growth', Brussels, 19.11.2025., https://commission.europa.eu/strategy-and-policy/policies/consumers/consumer-protection-policy/2030-consumer-agenda_en, 18 February 2026.
 5. Draft Proposal for the Amendments to the Consumer Protection Act, <https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=32306>, 19 February 2026
 6. Draft Proposal, Comments, <https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=32306>, 23 February 2026
 7. Draft Proposal, Art. 6., Comments, <https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=32306>, 23 February 2026
 8. Draft Proposal, Art. 27., Comments, <https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=32306>, 23 February 2026
 9. Draft Proposal, Art. 44., Comments, <https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=32306>, 23 February 2026
 10. <https://www.iusinfo.hr/zakonodavstvo/ZA2022B19A203>, Accessed 25 March 2026.
 11. 2025 Consumer Conditions Scoreboard, https://commission.europa.eu/document/download/2816337b-4fd1-4db2-a71c-d14a206a5a93_en?filename=consumer_conditions_scoreboard_2025_final.pdf, Accessed 25 March 2026.

UDK: 343.14 : 341.6
Review paper

Tea Micevska, PhD student

Faculty of Law „Justinianus Primus“, Ss. Cyril and Methodius University in Skopje,
Republic of North Macedonia

E-mail: t.micevska@pf.ukim.edu.mk

ORCID-ID: 0009-0003-6117-5058

ILLEGALLY OBTAINED EVIDENCE IN INTERNATIONAL ARBITRATION

ABSTRACT

The question of how to deal with illegally obtained evidence remains one of the most unsettled issues from both a theoretical and practical perspective. Despite the absence of a unified standard, such evidence continues to appear in arbitral proceedings. Thus, important questions about fairness, integrity and procedural flexibility are raised. What makes this topic particularly intriguing is the nature of arbitration itself, which is a system built on the free will of the parties. Yet, this very freedom generates a tension between fundamental principles, such as due process and good faith, on the one hand, and the inherent flexibility of arbitration on the other. This paper explores how relevant legal instruments and arbitral tribunals have approached this dilemma and considers whether there is room for at least a modest step toward a more consistent approach to the admissibility of such evidence in international arbitration.

Keywords: *international arbitration, illegally obtained evidence, practice, standard*

1. INTRODUCTION

In the absence of explicit rules and persistent prevailing approach, illegally obtained evidence almost invariably raises the same procedural question of whether it should be admitted or not. This imposes a burden on the process of adjudication. The decision ultimately turns on whether pursuit of truth should be prioritized for the cost of the illegal manner in which the evidence was obtained.

Arbitration is distinguished from judicial proceedings by its nature and characteristics. Parties choose arbitration as an alternative dispute resolution method due to its consensual foundation enabling party control over the resolution process, its procedural flexibility, as well as its perceived integrity. Thus, arbitration provides insight into a new dimension of the approach to illegally obtained evidence. On the one hand, in the lack of established rules, it may be argued that arbitrators enjoy greater discretion in the assessment of evidence obtained illegally. On the other hand, admitting illegally obtained evidence may be perceived as incitement to illegal activities which could impair some of

arbitration's greatest attributes – its reputation and integrity. Therefore, arbitrators seem to refer to fundamental principles, such as the good faith principle and equality of arms, when deciding whether such evidence should be admitted.

It is certain that there is no consensus on this matter, either from a theoretical or a practical perspective. Moreover, the rules of arbitral institutions provide no uniform answer. Nevertheless, the appearance of illegally obtained evidence in arbitral practice has allowed various tribunals to address these matters. Therefore, the first objective of this paper is to analyze the arbitration rules relating to the collection and admissibility of evidence, focusing on whether the use of illegally obtained evidence is regulated. In the absence of such rules, the aim is to identify the principles contained in the provisions which may serve as guidance for tribunals when deciding on its admissibility and use. Subsequently, an analysis will be conducted of several landmark arbitral awards in which the arbitrators addressed the use of such evidence. Due to the confidentiality of commercial arbitration, the focus of the research will be investment arbitration cases. The relevant cases are chosen because of their illustrative value in demonstrating diverse categories of illegality and consequently, various approaches to the admissibility of illegally obtained evidence. In order to identify underlying principles and patterns in arbitral practice, the analysis will focus on tribunals' reasoning and highlight the similarities and differences. The ultimate goal is to draw a conclusion regarding the tribunals' stance – whether it is consistent, justified and which specific characteristics define it.

2. LEGAL FRAMEWORK FOR ARBITRAL INSTITUTIONS REGARDING ADMISSIBILITY OF (ILLEGALLY) OBTAINED EVIDENCE

Owing to its flexibility, arbitration rules tend to ensure broad discretion in conducting the proceedings, including the taking of evidence, to the extent that parties may arguably be 'left in the dark' about the protection afforded to their rights when the use of illegally obtained evidence is in question.¹ When existent, the regulation of the evidence gathering and its admissibility is rather superficial, purposely leaving a gap for the parties to fill according to their disposition.² In the

¹ Diora Ziyaeva, Antonio Celso Pugliese Dentons, Hacking the system: admissibility of evidence from cyberattacks in arbitration, *Global Arbitration Review*, 18 July 2025, <https://globalarbitrationreview.com/review/the-arbitration-review-of-the-americas/2026/article/hacking-the-system-admissibility-of-evidence-cyberattacks-in-arbitration>, 23 February, 2026.

² *Ibid.*

See also: IBA Task Force for the Revision of the IBA Rules on the Taking of Evidence in International Arbitration, Commentary on the revised text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration, January 2021, p. 2, <https://www.ibanet.org/MediaHandler?id=4F797338-693E-47C7-A92A-1509790ECC9D>, 23 February, 2026.

course of analyzing different arbitration rules, they can be categorized into three different groups: (i) rules providing guided discretion, (ii) rules granting broad, but unguided discretion and (iii) rules categorized by regulatory silence.³

In the first group, the tribunals are encouraged, but not required to take certain evidentiary principles into account when determining the admissibility of evidence. A representative example is the American Arbitration Association's Commercial Arbitration Rules,⁴ which entitle the arbitrators with discretion in conducting arbitration, providing that 'the parties are treated with equality and that each party has the right to be heard and is given a fair opportunity to present its case'.⁵ The arbitrators shall determine, *inter alia*, the admissibility of the evidence and may exclude them if they deem to be 'cumulative or irrelevant',⁶ however, 'conformity to legal rules of evidence shall not be necessary'.⁷

In the second group, the rules give power to the tribunals to determine admissibility of evidence without express reference to applicable evidentiary rules. For example, the UNCITRAL Arbitration Rules⁸ prescribe that it shall, *inter alia*, determine the admissibility and weight of the evidence offered.⁹ This confirms that arbitrators are 'freed from having to observe the strict legal rules of evidence'.¹⁰ However, they should conduct the arbitration by treating the parties with equality, in a fair and efficient process in which they will be given a reasonable opportunity of presenting their case.¹¹ The PCA Arbitration Rules,¹² based on the 2010 UNCITRAL Arbitration Rules, also prescribe wide discretionary powers in determining the admissibility, relevance, materiality and weight of the evidence offered, while ensuring equality and fair treatment between the parties.¹³ The LCIA Rules¹⁴ give the arbitral tribunal the power 'to decide whether or not to apply

³ Ziyaeva, Dentons, *op.cit.* note 2.

⁴ American Arbitration Association's Commercial Arbitration Rules, <https://www.adr.org/rules-forms-and-fees/commercial/>, hereinafter: AAA Arbitration Rules.

⁵ AAA Arbitration Rules, R-33(a).

⁶ AAA Arbitration Rules, R-35(c),

⁷ AAA Arbitration Rules, R-35(a).

⁸ United Nations Commission on International Trade Law, UNCITRAL Arbitration Rules, Vienna, 2021, hereinafter: UNCITRAL Arbitration Rules.

⁹ UNCITRAL Arbitration Rules, Article 27.

¹⁰ Report of the Secretary-General: preliminary draft set of arbitration rules for optional use in ad hoc arbitration relating to international trade (UNCITRAL Arbitration Rules) (A/CN.9/97), Yearbook of the United Nations Commission on International Trade Law, Volume VI, 1975, p. 176.

¹¹ UNCITRAL Arbitration Rules, Article 17.

¹² Permanent Court of Arbitration, PCA Arbitration Rules with Optional Protocols adopted in 2024, <https://pca-cpa.org/en/services/arbitration-services/pca-arbitration-rules/>, hereinafter: PCA Arbitration Rules.

¹³ PCA Arbitration Rules, Articles 17 and 27.

¹⁴ London Court of International Arbitration, LCIA Rules 2020, https://www.lcia.org/Dispute_Resolution_Services/lcia-arbitration-rules-2020.aspx, hereinafter: LCIA Rules.

any strict rules of evidence (or any other rules) as to the admissibility, relevance or weight of any material tendered by a party on any issue of fact or expert opinion'.¹⁵ The SCC Arbitration Rules¹⁶ fall within this category of rules as well.¹⁷ Further, the SIAC Arbitration Rules¹⁸ take a similar approach and add that 'the Tribunal is not required to apply the rules of evidence of any applicable law in making such a determination'.¹⁹ The HKIAC Arbitration Rules also confer broad discretion upon the admissibility of evidence, 'including whether to apply strict rules of evidence'.²⁰ Thus, the arbitral tribunal has 'the power to admit or exclude any documents, exhibits or other evidence'.²¹ Under the ICSID framework, Article 43 of the ICSID Convention²² is the only provision that expressly addresses evidence, while the ICSID Arbitration Rules²³ (Rules 36–40) provide further procedural detail on the tribunal's handling of evidence.²⁴ Under these rules, the tribunal possesses a large measure of discretion – whether certain evidence should be admitted or excluded, whether certain weight should be given, whether it would prefer to see specific kind of evidence on any matter arising in the case.²⁵ However, the tribunals are not bound by any specific rules. The common ground for all of these rules is that they all give the Tribunals broad discretion in determining the admissibility of evidence, without referencing any specific rules. However, as a procedural safety net, some of the general provisions reflect adherence to some fundamental principles while conducting the arbitration. Consequently, as it will be demonstrated, the broad discretion of the tribunals becomes even broader when deciding on admissibility of illegally obtained evidence.

In the third group, the admissibility of evidence is not expressly regulated, and tribunal authority remains largely implicit. For example, the ICC Arbitration

¹⁵ LCIA Rules, Article 22.

¹⁶ Arbitration Rules of the SCC Arbitration Institute, Adopted by the Stockholm Chamber of Commerce and in force 1 January 2023, hereinafter: SCC Arbitration Rules.

¹⁷ SCC Arbitration rules, Article 31, para. 1: 'The admissibility, relevance, materiality, and weight of evidence shall be for the Arbitral Tribunal to determine.'

¹⁸ Arbitration Rules of the Singapore International Arbitration Centre SIAC Rules 7th Edition, 1 January 2025, <https://siac.org.sg/siac-rules-2025>, hereinafter: SIAC Arbitration Rules.

¹⁹ SIAC Arbitration Rules, Article 32.2.

²⁰ Hong Kong International Arbitration Centre, 2024 Administered Arbitration Rules, <https://hkiac.org/arbitration/rules-and-practice-notes/2024-administered-arbitration-rules/>, Article 22, hereinafter: HKIAC Arbitration Rules.

²¹ HKIAC Arbitration Rules, Article 22.

²² Convention on the settlement of investment disputes between States and nationals of other States, Washington, 1965, hereinafter: ICSID Convention.

²³ International Centre for Settlement of Investment Disputes (ICSID) (2022) ICSID Rules and Regulations. Washington, DC: World Bank Group.

²⁴ See: Schreuer's Commentary on the ICSID Convention: A Commentary on the Convention on the Settlement of Investment Disputes between States and Nationals of Other States. 3rd edn. Schill, S.W. et al. (eds.) Cambridge: Cambridge University Press, 2020, p. 909

²⁵ *Ibid*, p. 913.

Rules²⁶ only generally provide that the arbitral tribunal must conduct the arbitration fairly and impartially and guarantee 'that each party has a reasonable opportunity to present its case'.²⁷ The VIAC Arbitration Rules also fall under this category. They do not provide explicit admissibility rules in the sense of which kinds of evidence shall be rejected or accepted.²⁸ However, it is stipulated that 'the parties shall act in good faith, fairly and respectfully'.²⁹ Therefore, this category of evidence does not remotely regulate the admissibility of evidence, much less if they are obtained illegally.

It is evident that most of the rules do not address the use of illegally obtained evidence, but rather 'embrace broad permissive admissibility powers'.³⁰ Of course, it is not uncommon for national courts to use free evaluation when deciding on the (in)admissibility of certain evidence. However, in arbitration, this intentional gap may result in difficulties, especially due to opposing views of the parties, their different cultures or legal backgrounds.³¹ In an attempt to bridge the gap, the IBA Rules on Evidence were designed as a mechanism 'to supplement the legal provisions and the institutional, ad hoc or other rules that apply to the conduct of the arbitration'.³² Many investment and commercial arbitration tribunals agreed that they can serve as appropriate guidance, even in situations where the parties have not consented that they are formally applicable.³³ The Preamble itself calls upon fair process for the taking of evidence, conducted on the principle of good faith.³⁴ Further, the tribunal has the discretion to decide on the 'admissibility, relevance, materiality and weight of evidence'³⁵ and the power to exclude evidence in exhaustively enumerated cases.³⁶ However, the criteria for excluding

²⁶ International Chamber of Commerce, 2021 Arbitration Rules, <https://iccwbo.org/dispute-resolution/dispute-resolution-services/arbitration/rules-procedure/2021-arbitration-rules/#block-accordion-22>, ICC Arbitration Rules.

²⁷ ICC Arbitration Rules, Article 22 para. 4.

²⁸ See: VIAC Arbitration Rules, Articles 12 and 29.

²⁹ VIAC Arbitration Rules, Article 9, para. 5.

³⁰ Ashford, P., *The Admissibility of Illegally Obtained Evidence*, Arbitration, 2019, 85(4), p. 6.

³¹ IBA Task Force for the Revision of the IBA Rules on the Taking of Evidence in International Arbitration, Commentary on the revised text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration, January 2021, p. 2, <https://www.ibanet.org/MediaHandler?id=4F797338-693E-47C7-A92A-1509790ECC9D>, 23 February, 2026.

³² IBA Rules on the Taking of Evidence in International Arbitration, Adopted by a resolution of the IBA Council 17 December 2020 International Bar Association, <https://www.ibanet.org/MediaHandler?id=def0807b-9fec-43ef-b624-f2cb2af7cf7b>, Preamble, p. 7.

³³ Schreuer's Commentary on the ICSID Convention: A Commentary on the Convention on the Settlement of Investment Disputes between States and Nationals of Other States, p. 912, footnote 15: 'eg Metal-Tech v Uzbekistan, Award (4 October 2013) para 245'.

³⁴ IBA Rules on Evidence, Preamble.

³⁵ IBA Rules on Evidence, Article 9 para. 1.

³⁶ IBA Rules on Evidence, Article 9 para. 1: '(a) lack of sufficient relevance to the case or materiality to its outcome; (b) legal impediment or privilege under the legal or ethical rules determined by the Arbitral Tribunal to be applicable (see Article 9.4 below); (c)

evidence appears to be stringent, as the arbitral tribunal is responsible for conducting fair proceedings.³⁷ Nonetheless, the greatest novelty is that arbitral tribunals now 'may, at the request of a Party or on its own motion, exclude evidence obtained illegally'.³⁸ The Commentary of the revised text of the 2020 IBA Rules on Evidence,³⁹ provides one example: 'if the law of a country where a recording of a conversation was made prohibits recording conversations without permission of those involved, such recording may be considered to have been obtained illegally and therefore the tribunal may exclude it from the evidence.'⁴⁰ However, apart from this provision, the IBA Rules on Evidence do not provide guidelines or exemplary circumstances in which illegally obtained evidence should be excluded. This is due to the variations in national laws, as well as the variety in the arbitral tribunals' conclusions.⁴¹ Hence, the rules themselves make a gradation: the tribunal 'shall' exclude evidence in the situations provided for in Article 9(2), but 'may' exclude illegally obtained evidence under Article 9(3).

To sum up, most of the arbitration rules give broad discretion by providing that the arbitral tribunal shall determine the admissibility, relevance, materiality, and weight of the evidence without requiring any specific rules to be applied. Some arbitration rules refrain from even remotely establishing admissibility rules but provide that the whole arbitral process should be conducted according to the principles of fairness and equality of the parties. In any case, the IBA Rules on Evidence can be applied supplementarily. The provision stipulating that illegally obtained evidence 'may' be excluded attests to its presence in practice. However, since the provision is scarce, it is far from clarifying its use to any meaningful extent.

Therefore, it is necessary to make an overview of the practice in which illegally obtained evidence has appeared and the approaches which the tribunals have

unreasonable burden to produce the requested evidence; (d) loss or destruction of the Document that has been shown with reasonable likelihood to have occurred; (e) grounds of commercial or technical confidentiality that the Arbitral Tribunal determines to be compelling; (f) grounds of special political or institutional sensitivity (including evidence that has been classified as secret by a government or a public international institution) that the Arbitral Tribunal determines to be compelling; or (g) considerations of procedural economy, proportionality, fairness or equality of the Parties that the Arbitral Tribunal determines to be compelling.'

³⁷ Ahern William, Admissibility of Evidence, 2025, https://jusmundi.com/en/document/publication/en-admissibility-evidence?login_success=true&login_success=true&login_success=true&login_success=true, 23 February, 2026.

³⁸ IBA Rules on Evidence, Article 9 para. 3.

³⁹ IBA Task Force for the Revision of the IBA Rules on the Taking of Evidence in International Arbitration, Commentary on the revised text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration, January 2021, p. 30, <https://www.ibanet.org/MediaHandler?id=4F797338-693E-47C7-A92A-1509790ECC9D>, 23 February, 2026.

⁴⁰ Ibid.

⁴¹ Ibid.

adopted addressing them. The following analysis of selected investment arbitration awards illustrates how various tribunals apply different principles in practice.

3. ARBITRAL TRIBUNALS' APPROACH IN PRACTICE

Another consequence of the tribunal's flexibility and wide discretion is the absence of unified approach when assessing (illegally obtained) evidence.⁴² By making an overview of the leading cases which dealt with this matter, it is important to identify the principles they used in reaching their decisions.

A pivotal case which initially set the contours in the context of illegally obtained evidence in arbitration is *Methanex Corporation v United States of America* (*Methanex v USA*).⁴³ Methanex alleged that the State of California's environmental regulation infringed upon its NAFTA-guaranteed investment treaty rights.⁴⁴ It therefore hired a private investigator who obtained documents by trespassing on a private property and conducting 'dumpster-diving' activities in internal trashcans.⁴⁵ This was an ongoing operation carried out over a period of months. Documentation contained private correspondence, materials subject to legal professional privilege, personal notes and a private address-book.⁴⁶ Having established *prima facie* that the evidence was obtained unlawfully, the USA shifted the burden of proof to Methanex, which did not demonstrate the lawfulness of the documents' acquisition.⁴⁷ In the final award, the Tribunal held that the documents obtained before the proceedings began were in violation of the general duty of good faith which is 'incumbent on all who participate in international arbitration'.⁴⁸ The documents obtained after the commencement of the proceedings, aside from violating the principle of good faith, also offended the 'principles of justice and fairness required of all parties in every international arbitration'.⁴⁹ Thus, the Tribunal held that the evidence was of 'marginal evidential

⁴² See: Ahern William, *Admissibility of Evidence*, 2025, https://jusmundi.com/en/document/publication/en-admissibility-evidence?login_success=true&login_success=true&login_success=true&login_success=true, 23 February, 2026.

⁴³ *Methanex Corporation v United States*, Final Award on Jurisdiction and Merits, (2005) 44 ILM 1345, Inside US Trade, 19 August 2005, 12, IIC 167 (2005), 3rd August 2005, Ad Hoc Tribunal (UNCITRAL), hereinafter: *Methanex v USA*.

⁴⁴ *Methanex v USA*, para. 2.

⁴⁵ *Methanex v USA*, para. 37: 'Mr McAnish stated that, every weekday morning at about 6.00 a.m., he visited the building and accessed the dumpsters from the public walkway in front of the doors to the dumpster area. He stated that the doors were never locked and, at times, were open or ajar.'; Ashford, *op. cit.* note 31, p.7.

⁴⁶ *Methanex v USA*, para. 4.

⁴⁷ *Methanex v USA*, para. 55.

⁴⁸ *Methanex v USA*, para. 58.

⁴⁹ *Methanex v USA*, para. 59.

significance in support of Methanex's case.⁵⁰ This is an example of a direct involvement of the party in illegal evidence gathering.

Another case demonstrating party involvement is EDF v Romania,⁵¹ where the Claimant knew and agreed to illegally record a conversation with a Romanian witness, therefore violating her right to privacy.⁵² Relying upon the findings in Methanex v USA, the tribunal held that admitting the secretly recorded audio tape 'would be contrary to the principles of good faith and fair dealing required in international arbitration'.⁵³ Thus, the audiotape was incomplete, as it was missing a portion of the original soundtrack, which raised authenticity concerns. This was another reason for not admitting it as evidence.⁵⁴ Interestingly enough, although the Tribunal emphasized that admission of evidence in arbitration is governed by international law, it found that the taping was unlawful under Romanian law, as it breached the right to privacy.⁵⁵ Referring to the Corfu Channel Case, as a leading case in this matter, the Tribunal underlined 'that admissibility of unlawfully obtained evidence is to be evaluated in the light of the particular circumstances of the case, as in the case of the ICJ Judgment in the Corfu Channel Case'.⁵⁶

Another example of a party involvement is Libananco Holdings Co. Limited v. Republic of Turkey.⁵⁷ The Respondent, while exercising its sovereign powers to obtain evidence in a criminal investigation, accessed 'hundreds, or even thousands', of communications with the Claimant's counsel and potential witnesses.⁵⁸ Although Turkey argued that the aim of the surveillance was to prevent money laundering, the Tribunal held that it 'could not allow its process to be used as the cover for a mere fishing expedition'.⁵⁹ It therefore weighed procedural fairness, confidentiality, legal privilege and parties' immunities against Turkish sovereign policing powers.⁶⁰ It called upon the parties' obligation to

⁵⁰ Methanex v USA, para. 56.

⁵¹ EDF (Services) Limited v. Romania, ICSID Case No. ARB/05/13.

⁵² S Ng, N., *Illegally Obtained Evidence in International Arbitration: Protecting the Integrity of the Arbitral Process*, Singapore Academy of Law Journal 32, no. 2, September 2020, 747-770, p. 754.

⁵³ EDF (Services) Limited v. Republic of Romania, ICSID Case No. ARB/05/13, Procedural Order No. 3, para. 38. More precisely, the Tribunal referred to the IBA Rules, Article 9, para. 2(g).

⁵⁴ Gupta, K., *Admissibility of Unlawfully Obtained Evidence in International Arbitration*, NLIU Law Review, Issue II, Vol XI, 2022, p. 101.

⁵⁵ EDF (Services) Limited v. Republic of Romania, ICSID Case No. ARB/05/13, Procedural Order No. 3, para. 36, 47.

⁵⁶ EDF (Services) Limited v. Republic of Romania, ICSID Case No. ARB/05/13, Procedural Order No. 3, para. 38.

⁵⁷ Libananco Holdings Co. Limited v. Republic of Turkey, ICSID Case No. ARB/06/8, hereinafter: Libananco v Turkey.

⁵⁸ Libananco Holdings Co. Limited (Claimant) v the Republic of Turkey (Respondent) (ICSID Case No. ARB/06/8), Decisin on Preliminary Issues, 23 June 2008, para. 72, hereinafter Libananco v Turkey, Decisin on Preliminary Issues, 23 June 2008.

⁵⁹ *Ibid*, para. 70.

⁶⁰ *Ibid*, para. 78.

arbitrate fairly and in good faith.⁶¹ It was ordered that the Respondent not 'intercept or record communications between legal counsel for the Claimant on the one hand and representatives of the Claimant and other persons in Turkey on the other hand';⁶² to destroy all intercepted emails and communications which in any way related to the arbitration;⁶³ to exclude all privileged documents and information which have been disclosed to the Tribunal;⁶⁴ that the Respondent must ensure that no information or documents obtained by 'its criminal investigation authorities shall be made available to any person having any role in the defense of this arbitration'.⁶⁵ This is a rather firm standing on the protection of confidential and privileged information for a party, although, arguably, not applied equally to both categories.⁶⁶ In the case, some of the audio recordings were not admitted as 'neither of the Parties' experts was able to confirm that the audio recordings in question were authentic'.⁶⁷

In *Caratube International Oil Company LLP and Devincci Salah Hourani v. Republic of Kazakhstan* (*Caratube v Kazakhstan*), a slightly different approach was taken. Firstly, the case demonstrates that if the evidence or information is publicly accessible, there is limited basis for excluding it from consideration.⁶⁸ Namely, Caratube initiated the arbitral proceedings due to an alleged seizure of their oil exploration and production rights. The Tribunal had to decide on the admissibility of eleven documents which were hacked and leaked on 'Kazakhleaks' alongside 60,000 other documents. The Claimant argued that the Tribunal could not be "placed in a sterile environment or a bubble detached from the real world and ignore these documents or pretend they don't exist".⁶⁹ The Respondent, on the other hand, contended that the documents are infringing the principle of equality of arms and legal privilege. Nevertheless, the Tribunal successfully illustrated that

See also: Ireton, J., *The Admissibility of Evidence in ICSID Arbitration: Considering the Validity of WikiLeaks Cables as Evidence*, ICSID Review, Vol. 30, No. 1, 2015, doi:10.1093/icsidreview/siu029, p. 238; Bertrou, G., Alekhin, S., *The Admissibility of Unlawfully Obtained Evidence in International Arbitration: Does the End Justify the Means?*, Les Cahiers de l'Arbitrage, 2018-4, pp. 11-71.

⁶¹ *Libananco v Turkey*, Decisin on Preliminary Issues, 23 June 2008, para. 78.

⁶² *Ibid*, para. 82, 1.1.1.

⁶³ *Ibid*, para. 82, 1.1.3.

⁶⁴ *Ibid*, para. 82, 1.1.6.

⁶⁵ *Ibid*, para. 82, 1.2.

⁶⁶ Ireton, *op. cit.* note 61, p. 238; Bertrou, Alekhin, *op. cit.* note 61, p. 29.

⁶⁷ *Libananco Holdings Co. Limited v. Republic of Turkey*, ICSID Case No. ARB/06/8, Award, 2 Sept 2011, para. 383.

⁶⁸ Sahu, R. K., *Inadmissible but irresistible: navigating standards of admissibility of illegally obtained evidence against an arbitrator*, International Arbitration Law Review, 2025, 28(1), p. 2.

⁶⁹ Alison Ross, Tribunal rules on admissibility of hacked Kazakh emails, September 2015, <https://globalarbitrationreview.com/article/tribunal-rules-admissibility-of-hacked-kazakh-emails>.

it is possible to split the illegally obtained evidence into admissible and rejected.⁷⁰ It held that the risk of an award that would be "artificial and factually wrong when considered in light of the publicly available information" was considered to outweigh concerns relating to cybercrime and potential unfairness and admitted the non-privileged documents.⁷¹ However, four privileged documents were rejected, as the lawyer-client privilege was not waived with the hacking of the documents and could only be disregarded in "rather extreme circumstances."⁷²

ConocoPhillips v Venezuela is a case in which, *inter alia*, a total of three requests of reconsideration of the Decision on jurisdiction and merits⁷³ and two reconstitutions of the tribunal took place. After rendering the award, Wikileaks cables were submitted as evidence on behalf of the Respondent. In their Request for reconsideration, they requested a new hearing in light of the new facts discovered in the cables, proving that contrary to the findings in the decision, the Respondent negotiated in good faith with the Claimant. The Tribunal denied their request, stating that it does not have the power to open up the award.⁷⁴ In his dissenting opinion, Professor Abi-Saab contested to the tribunal's decision as it follows: "In these circumstances, I don't think that any self-respecting Tribunal that takes seriously its overriding legal and moral task of seeking the truth and dispensing justice according to law on that basis, can pass over such evidence, close its blinkers and proceed to build on its now severely contestable findings, ignoring the existence and the relevance of such glaring evidence. It would be shutting itself off by an epistemic closure into a subjective make believe world of its creation; a virtual reality in order to fend off probable objective reality; a legal comedy of errors on the theatre of the absurd, not to say travesty of justice, that makes mockery not only of ICSID arbitration but of the very idea of adjudication."⁷⁵ Shortly after Professor Abi-Saab's resignation, the Respondent submitted a new request for reconsideration which was rejected on the same

⁷⁰ Drahanov, D., *The issue of admissibility of evidence in the investment arbitration Should the tribunal use hacked and illegal documentation?*, Master Thesis, Uppsala Universitet, 2019, p. 30.

⁷¹ Bertrou, Alekhin, *op. cit.* note 61, p. 35.

⁷² Although the Tribunal noted that the rejection of the privileged documents could lead to a "regrettable but inescapable and acceptable" risk of an ultimate decision "inconsistent with the privileged leaked documents in the public domain.", *Ibid.*

⁷³ ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela, ICSID Case No. ARB/07/30, 13 December 2007.

⁷⁴ ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela (ICSID Case No. ARB/07/30), Decision on Respondent's Request for Reconsideration, March 10, 2014, para. 22.

⁷⁵ Professor Abi-Saab's Dissenting Opinion to Decision on Jurisdiction and Merits dates February 19, 2015, nearly 1.5 years after the date of the underlying Decision. As explained in the introductory paragraphs of the Dissenting Opinion, the delay was caused by Professor Abi-Saab's ill health (ConocoPhillips Dissenting Opinion of Georges Abi-Saab, para. 2).

procedural grounds.⁷⁶ Professor Bucher, in line with his predecessor, Professor Abi-Saab, highlighted in his Dissenting opinion that the tribunal had power to reconsider its previous decision based on the newly discovered facts.⁷⁷ After the resignation of the Tribunal's Chairman, the Respondent submitted its third request for reconsideration, which was once again rejected. Intriguingly enough, the Tribunal emphasized that the leaked cables were "not always easy to understand", even though it did not elaborate on its (in)admissibility. This is peculiar, considering that international arbitration is characterized with decisions 'of staggering length in which every argument raised by the parties is often reproduced verbatim in the body of the award'.⁷⁸ The illegality of the documents was not objected to by the Claimant either. Therefore, one cannot help but wonder whether, if the evidence had been presented in a timely manner, the tribunal might not have objected to it.⁷⁹

In the landmark Yukos arbitrations,⁸⁰ the Tribunal heavily relied on confidential diplomatic cables from the US State Department that were made public by WikiLeaks.⁸¹ This was to prove that the Respondent exerted pressure on Claimant's auditor 'to withdraw the audits in order to bolster the legitimacy of the destruction of Yukos'.⁸² However, the Respondent did not dispute the admissibility or authenticity of said evidence and neither did the Tribunal take explicit position on the matter.

From the overview, it can be seen that illegally obtained evidence is not automatically inadmissible. Two dominant circumstances that tribunals take into account are the involvement of the parties in obtaining the evidence and its availability in the public domain. At the same time, due to the specificities of each individual case, additional factors are also considered. For example, *Methanex v the USA*, *EDF v Romania* and *Libananco v Turkey* are cases in which the parties

⁷⁶ *ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela* (ICSID Case No. ARB/07/30), Decision on the Respondent's Request for Reconsideration, February 9, 2016, para. 27-28, 37.

⁷⁷ *ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela* (ICSID Case No. ARB/07/30), Dissenting Opinion by Arbitrator Andreas Bucher, February 9, 2016, para. 34; Bertrou, Alekhin, *op. cit.* note 61 p. 32.

⁷⁸ Boykin, J. H., Havalic, M., *Fruits of the Poisonous Tree: The Admissibility of Unlawfully Obtained Evidence in International Arbitration*, October 2014, https://www.iadclaw.org/assets/1/7/6_Bassiri_Boykin_and_Havalic_Fruits_of_the_Poisonous_Tree_-_Admissibility_of_Unlawfully_Obtained_Evidence.pdf, 23 February, 2026, p. 9.

⁷⁹ Drahanov, *op. cit.* note 71, p. 33.

⁸⁰ *Yukos Universal Limited (Isle of Man) v. The Russian Federation*, PCA Case No. 2005-04/AA227, hereinafter *Yukos v Russia*; *Hulley Enterprises Ltd. v. Russian Federation*, PCA Case No. 2005-03/AA226; *Veteran Petroleum v. Russian Federation*.

⁸¹ Blair, C., Vidak Gojkovic, E., *WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence*, ICSID Review, ICSID Review - Foreign Investment Law Journal, Volume 33, Issue 1, Winter 2018.

⁸² *Yukos v Russia*, H. The Withdrawal of PWC's Audit Opinions.

themselves were involved in obtaining the evidence. However, despite this shared characteristic, the tribunals relied on different considerations in determining inadmissibility, particularly in *Libananco v Turkey*, where the tribunal balanced the competing interests of the parties in assessing admissibility. A common feature in *Caratube v Kazakhstan*, *ConocoPhillips v Venezuela* and *Yukos* is the availability of the evidence in the public domain, which constitutes a particularly relevant factor in favour of admissibility. Nevertheless, this too does not amount to a general rule, as tribunals in each case take into account different circumstances leading to different outcomes. For instance, *Caratube v Kazakhstan* suggests that privileged documents occupy a 'qualified position' compared to other types of evidence, while *ConocoPhillips v Venezuela* and *Yukos* leave the question of admissibility open: in the former, inadmissibility is based on procedural preclusion for late submission of evidence rather than a substantive assessment of the issue, whereas in the latter the matter is not addressed at all.

It follows that there is neither a uniform approach nor a consistent methodology in the tribunals' reasoning. Moreover, even when invoking specific grounds, it remains unclear how illegally obtained evidence violates the principles relied upon by the tribunals. Therefore, while such evidence is evidently present in arbitral practice and certain lines of reasoning have begun to emerge, these do not yet amount to a coherent approach. Nonetheless, they signal a gradual evolution toward greater consistency in the future.

4. CONCLUSION

In light of the analyzed provisions and the case-law of the arbitral tribunals, two main conclusions may be drawn.

Firstly, the arbitration rules generally confer broad discretionary powers to tribunals to determine admissibility of evidence. Although some of the rules give tribunals authority to exclude the evidence, none of them stipulate illegally obtained evidence as a ground for exclusion. The IBA Rules on Evidence, as a soft law instrument, introduced an important novelty, namely that tribunals may exclude evidence obtained in an illegal manner. However, the application of this rather vague and broadly formulated provision will continue to depend on the specific circumstances of each case and the tribunal's approach, much as it did prior to its adoption.⁸³

Secondly, the overview of the landmark cases in this area demonstrates some patterns, *i.e.* overlapping elements and principles that the Tribunals rely upon. Regarding the common elements, it can be seen that: illegally obtained evidence are not automatically excluded from the proceedings; it is particularly important

⁸³ See: Khodykin, R., Mulcahy, C., and Fletcher, N., *A Guide to the IBA Rules on the Taking of Evidence in International Arbitration*, Oxford Law Pro, 2019, <https://doi.org/10.1093/law/9780198818342.001.0001>, p. 415.

whether the party itself was involved in the illegal obtaining of the evidence or if it was obtained by a third party; arbitrators take into consideration whether the documents are publicly available; and privileged documents constitute a category of evidence which enjoy special protection. With respect to the applied principles, the Tribunals usually rely upon basic fundamental principles, such as good faith, fairness and equality of arms, justice, confidentiality, privilege, as well as the right to privacy of the parties, materiality or authenticity of evidence. However, their invocation often remains abstract and inconsistently applied, without clearly demonstrating how the illegally obtained evidence infringes upon them.

Accordingly, given the wide discretion conferred by the applicable rules and in view of the approaches adopted by tribunals in practice, the most appropriate guiding framework directed towards a more coherent methodological approach would be the following three-step test:

- (i) Has the evidence been obtained unlawfully by a party who seeks to benefit from it?
- (ii) Does public interest favor rejecting the evidence as inadmissible?⁸⁴
- (iii) Do the interests of justice favor the admission of evidence?⁸⁵

However, Tribunals would still have to consider the authenticity, reliability and persuasiveness of the evidence, especially in times of high technological development.⁸⁶ Additionally, the test should be applied cautiously, evaluating each step individually and in combination, taking into consideration the circumstances of the case. The proposed test may be used as a flexible analytical tool for different procedural contexts that helps tribunals decide on the admissibility of evidence and determine the weight and probative value to be given to such evidence when necessary. Namely, a mechanical application could lead to risks in practice. As it was demonstrated by the case-law, tribunals generally exclude evidence that is privileged or illegally obtained by the party itself, while confidential evidence and evidence obtained from third parties is usually admitted. Therefore, in some cases, the party's involvement shouldn't be the sole decisive reason for excluding the evidence. This should not be understood as encouraging wrongdoing, because excluding highly important facts and evidence could undermine the fairness of the proceedings.⁸⁷ All of the circumstances of the case must be carefully considered, in order to avoid, in the words of Professor Ali-Saab - 'travesty of justice'. This approach shall be seen as a guide to balance the need to uphold procedural fairness while avoiding rigid rules that could exclude important evidence.

⁸⁴ Example: legal privilege (attorney-client communications), diplomatic immunity and inviolability, state secrecy, see: Blair, Vidak Gojkovic, *op. cit.* note 82, p. 257.

⁸⁵ The 3-step test is proposed by Cherie Blair and Ema Vidak Gojkovic, see: Blair, Vidak Gojkovic, *op. cit.* note 82.

⁸⁶ Example: principles of fairness, justice, procedural integrity, equality of arms, *Ibid*, p. 257, 259.

⁸⁷ *Ibid*, p. 258.

REFERENCES

BOOKS AND ARTICLES

1. Ashford, P., *The Admissibility of Illegally Obtained Evidence*, Arbitration, 2019, 85(4), 377-387
2. Bertrou, G., Alekhin, S., *The Admissibility of Unlawfully Obtained Evidence in International Arbitration: Does the End Justify the Means?*, Les Cahiers de l'Arbitrage, 2018-4, 11-71
3. Blair, C., Vidak Gojkovic, E., *WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence*, ICSID Review, ICSID Review - Foreign Investment Law Journal, Volume 33, Issue 1, Winter 2018, 235-259
4. Boykin, J. H., Havalic, M., *Fruits of the Poisonous Tree: The Admissibility of Unlawfully Obtained Evidence in International Arbitration*, October 2014, https://www.iadclaw.org/assets/1/7/6_Bassiri_Boykin_and_Havalic_Fruits_of_the_Poisonous_Tree_-_Admissibility_of_Unlawfully_Obtained_Evidence.pdf, 23 February, 2026
5. Drahanov, D., *The issue of admissibility of evidence in the investment arbitration Should the tribunal use hacked and illegal documentation?*, Master Thesis, Uppsala Universitet, 2019, p. 30
6. Gupta, K., *Admissibility of Unlawfully Obtained Evidence in International Arbitration*, NLIU Law Review, Issue II, Vol XI, 2022, 86-109
7. IBA Task Force for the Revision of the IBA Rules on the Taking of Evidence in International Arbitration, *Commentary on the revised text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration*, January 2021, <https://www.ibanet.org/MediaHandler?id=4F797338-693E-47C7-A92A-1509790ECC9D>
8. Ireton, J., *The Admissibility of Evidence in ICSID Arbitration: Considering the Validity of WikiLeaks Cables as Evidence*, ICSID Review, Vol. 30, No. 1, 2015, doi:10.1093/icsidreview/siu029, 231-242
9. Khodykin, R., Mulcahy, C., and Fletcher, N., *A Guide to the IBA Rules on the Taking of Evidence in International Arbitration*, Oxford Law Pro, 2019, <https://doi.org/10.1093/law/9780198818342.001.0001>
10. Report of the Secretary-General: preliminary draft set of arbitration rules for optional use in ad hoc arbitration relating to international trade (UNCITRAL Arbitration Rules) (A/CN.9/97), Yearbook of the United Nations Commission on International Trade Law, Volume VI, 1975
11. S Ng, N., *Illegally Obtained Evidence in International Arbitration: Protecting the Integrity of the Arbitral Process*, Singapore Academy of Law Journal 32, no. 2, September 2020, 747-770

12. Sahu, R. K., *Inadmissible but irresistible: navigating standards of admissibility of illegally obtained evidence against an arbitrator*, International Arbitration Law Review, 2025, 28(1), 45-51
13. Schreuer's Commentary on the ICSID Convention: A Commentary on the Convention on the Settlement of Investment Disputes between States and Nationals of Other States. 3rd edn. Schill, S.W. et al. (eds.) Cambridge: Cambridge University Press, 2020

LEGAL RULES

1. Arbitration Rules of the SCC Arbitration Institute, Adopted by the Stockholm Chamber of Commerce and in force 1 January 2023 , <https://sccarbitrationinstitute.se/en/scc-arbitration-rules-english-2023/>
2. Arbitration Rules of the Singapore International Arbitration Centre SIAC Rules 7th Edition, 1 January 2025, <https://siac.org.sg/siac-rules-2025>
3. Convention on the settlement of investment disputes between States and nationals of other States, Washington, 1965
4. Hong Kong International Arbitration Centre, 2024 Administered Arbitration Rules, <https://hkiac.org/arbitration/rules-and-practice-notes/2024-administered-arbitration-rules/>
5. IBA Rules on the Taking of Evidence in International Arbitration, Adopted by a resolution of the IBA Council 17 December 2020 International Bar Association, <https://www.ibanet.org/MediaHandler?id=def0807b-9fec-43ef-b624-f2cb2af7cf7b>
6. International Centre for Settlement of Investment Disputes (ICSID) (2022) ICSID Rules and Regulations. Washington, DC: World Bank Group
7. International Chamber of Commerce, 2021 Arbitration Rules, <https://iccwbo.org/dispute-resolution/dispute-resolution-services/arbitration/rules-procedure/2021-arbitration-rules/#block-accordion-22>
8. London Court of International Arbitration, LCIA Rules 2020, https://www.lcia.org/Dispute_Resolution_Services/lcia-arbitration-rules-2020.aspx
9. Permanent Court of Arbitration, PCA Arbitration Rules with Optional Protocols adopted in 2024, <https://pca-cpa.org/en/services/arbitration-services/pca-arbitration-rules/>
10. United Nations Commission on International Trade Law, UNCITRAL Arbitration Rules, 2021

COURT PRACTICE

1. ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela (ICSID Case No. ARB/07/30), Respondent's Letter to Tribunal Regarding Decision on Jurisdiction and Merits, September 8, 2013
2. ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela (ICSID Case No. ARB/07/30), Decision on the Respondent's Request for Reconsideration, February 9, 2016
3. ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela (ICSID Case No. ARB/07/30), Dissenting Opinion by Arbitrator Andreas Bucher, February 9, 2016
4. EDF (Services) Limited v. Republic of Romania, ICSID Case No. ARB/05/13, Procedural Order No. 3
5. EDF (Services) Limited v. Romania, ICSID Case No. ARB/05/13
6. Hulley Enterprises Ltd. v. Russian Federation, PCA Case No. 2005-03/AA226
7. Libananco Holdings Co. Limited (Claimant) and the Republic of Turkey (Respondent) (ICSID Case No. ARB/06/8), Decisin on Preliminary Issues, 23 June 2008
8. Libananco Holdings Co. Limited v. Republic of Turkey, ICSID Case No. ARB/06/8
9. Libananco Holdings Co. Limited v. Republic of Turkey, ICSID Case No. ARB/06/8, Award, 2 Sept 2011
10. Methanex Corporation v United States, Final Award on Jurisdiction and Merits, (2005) 44 ILM 1345, Inside US Trade, 19 August 2005, 12, IIC 167 (2005), 3rd August 2005, Ad Hoc Tribunal (UNCITRAL)
11. Yukos Universal Limited (Isle of Man) v. The Russian Federation, PCA Case No. 2005-04/AA227

NETWORK RESOURCES

1. Ahern William, Admissibility of Evidence, 2025, https://jusmundi.com/en/document/publication/en-admissibility-evidence?login_success=true&login_success=true&login_success=true&login_success=true, 23 February, 2026
2. Alison Ross, Tribunal rules on admissibility of hacked Kazakh emails, September 2015, <https://globalarbitrationreview.com/article/tribunal-rules-admissibility-of-hacked-kazakh-emails>, 23 February 2026

3. Diora Ziyaeva and Antonio Celso Pugliese Dentons, 'The Arbitration Review of the Americas, Hacking the system: admissibility of evidence from cyberattacks in arbitration', Global Arbitration Review, 18 July 2025, <https://globalarbitrationreview.com/review/the-arbitration-review-of-the-americas/2026/article/hacking-the-system-admissibility-of-evidence-cyberattacks-in-arbitration>

UDK: 342.4 : 347.991 (497.5)
341.645

Preliminary communication

Sanja Čović Jurčević, PhD student
Faculty of Law, University of Split, Croatia
E-mail: sanja.covic.jurcevic@pravst.hr
ORCID-ID: 0000-0002-1926-2831

COSTS OF PROCEEDINGS BEFORE THE CONSTITUTIONAL COURT AND THE RIGHT OF ACCESS TO A COURT IN THE LIGHT OF ECtHR CASE LAW *

ABSTRACT

This paper examines whether the Croatian Constitutional Court's approach to the reimbursement of costs incurred in constitutional complaint proceedings may constitute a disproportionate financial barrier and thereby impair the right of access to a court under Article 6(1) of the European Convention on Human Rights. While domestic law (Article 23 of the Constitutional Act on the Constitutional Court) establishes the general rule that each participant bears their own costs, the European Court of Human Rights (ECtHR) has clarified that a formalistic refusal to reimburse costs—particularly where the complainant has been successful and the costs represent a serious burden—may undermine the very essence of the right of access to a court. Using a doctrinal and case-law analysis, the paper first outlines the Convention standards on access to a court and financial restrictions, then provides a statistical overview of applications against Croatia before the ECtHR, and finally focuses on the ECtHR judgments in Dragan Kovačević v. Croatia and Moskalj v. Croatia as well as the subsequent shift in the Constitutional Court's practice (notably decision U-III-3686/2019 and later cases). The analysis shows that the decisive element is a context-sensitive proportionality assessment, taking into account the nature and importance of the case, the complainant's vulnerability, and their financial situation. The paper argues that the post-Kovačević approach strengthens predictability and aligns Croatian constitutional adjudication with Convention requirements, thereby enhancing the effectiveness of constitutional complaint proceedings as a domestic remedy.

Keywords: *Constitutional Court of the Republic of Croatia, constitutional complaint costs, reimbursement of costs, proportionality test, ECtHR case law*

* This paper is a product of work that has been fully supported by the Faculty of Law, University of Split, under the project nr. 2. „Civil Procedural Law – current state and future tendencies (HR-GPP)“.

1. INTRODUCTION TO THE EUROPEAN CONVENTION ON HUMAN RIGHTS AND THE EUROPEAN COURT OF HUMAN RIGHTS

Today, numerous international instruments are applied at the international level for the protection of human rights and fundamental freedoms. One of the most significant among them, indeed, arguably the cornerstone of the European human rights system, is the European Convention on Human Rights (ECHR)¹. The ECHR was adopted with the aim of safeguarding civil, political, social and economic rights. It entered into force on 3 September 1953, following its ratification by the first twelve States. Although the original text of the ECHR has never been amended, its provisions have been supplemented through additional Protocols². The Republic of Croatia ratified the ECHR, together with its Protocols, on 5 November 1997.

Moreover, the ECHR has become the keystone of the European political framework precisely because the execution of every judgment of the European Court of Human Rights (ECtHR)³ in which a respondent State has been found to have violated the ECHR, as well as every decision on a friendly settlement between the respondent State and the applicant, is carefully and systematically supervised by the other High Contracting Parties through their representation in the Committee of Ministers of the Council of Europe, the principal decision-making body of that international organisation established by its Statute.^{4 5}

Although the ECHR represents one of the most important legal instruments for the protection of human rights, its true significance primarily derives from the work

¹ European Convention for the Protection of Human Rights and Fundamental Freedoms, consolidated text, Official Gazette – International Treaties Nos. 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10, 13/17 (hereinafter: "Convention" or "ECHR"). See more in: Maričić, D., *Konvencija za zaštitu temeljnih prava i sloboda*, Novi informator, Zagreb 2012.

² European Convention on Human Rights as amended by Protocols Nos. 11, 14 and 15 and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, available at: https://www.echr.coe.int/documents/convention_bos.pdf, accessed 15 January 2026.

³ European Court of Human Rights (hereinafter: "ECtHR").

⁴ Omejec, J., *Execution of Judgments and Decisions of the European Court of Human Rights*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 62, No. 5–6/2012, p. 1915.

⁵ Statute of the Council of Europe, ETS No. 001, opened for signature 5 May 1949, entered into force 3 August 1949. Consolidated text available at: Council of Europe Treaty Office, <http://conventions.coe.int/Treaty/en/Treaties/Html/001.htm> See also: Council of Europe, A Unique and Effective Mechanism – Execution of Judgments of the European Court of Human Rights, http://www.coe.int/t/dghl/monitoring/execution/Presentation/Default_en.asp, accessed 15 January 2026.

and case law of the Court established for that purpose. The ECtHR was established in 1959; however, at that time individuals were not able to apply directly to the Court, but only through the European Commission of Human Rights. A major institutional reform occurred with the entry into force of Protocol No. 11, which abolished the Commission and introduced the possibility of direct individual applications to the Court. Since the entry into force of that Protocol, States ratifying the ECHR automatically recognise the jurisdiction of the ECtHR and undertake to abide by its final judgments in any case to which they are parties.⁶

As already noted, the importance of the ECHR does not lie solely in the enumeration of rights guaranteed in its substantive provisions; rather, it stems from the Court's jurisprudence, which defines contemporary standards of human rights protection in the member States. The ECtHR has emphasised that the purpose of its judgments is not merely to resolve individual disputes brought before it, but also to clarify, safeguard and develop the rules established by the ECHR.⁷

With regard to the jurisdiction of the Court, several points should be emphasised. The ECtHR examines only those applications alleging violations of rights guaranteed by the ECHR and its Protocols.⁸ The ECtHR is not a court of appeal against decisions of domestic courts and therefore has no authority to annul or amend national judgments. Its judgments are declaratory in nature. The purpose of the protection afforded by Article 6(1) of the ECHR is to ensure the fairness of proceedings, not to review the correctness of the outcome reached in a particular case. Accordingly, the ECtHR will regularly declare inadmissible as manifestly ill-founded those applications in which applicants primarily seek to challenge the domestic courts' assessment of facts or interpretation of law, reiterating that it is not its role to act as a "fourth instance" tribunal.⁹

The interpretation and application of national law fall primarily within the competence of domestic authorities, not the ECtHR. However, in assessing whether the proceedings as a whole were fair, the ECtHR necessarily takes into

⁶ The ECtHR ensures the observance of the engagements undertaken by the High Contracting Parties in the Convention. The Court is composed of a number of judges equal to the number of Contracting States (currently forty-six). Judges sit in their individual capacity and are elected for a non-renewable term of nine years. See more at: <https://uredzastupnika.gov.hr/europski-sud-za-ljudska-prava/186>, accessed 5 January 2026.

⁷ *Loizidou v. Turkey*, no. 15318/89, judgment of 28 November 1996; *Sejdić and Finci v. Bosnia and Herzegovina*, nos. 27996/06 and 34836/06, judgment of 22 December 2009.

⁸ Applications not fulfilling Convention requirements are declared inadmissible.

⁹ Uzelac, A., *The Right to a Fair Trial in Civil Matters: New Case Law of the European Court of Human Rights and Its Influence on Croatian Law and Practice*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 60, No. 1/2010, pp. 101–148, p. 106.

account the manner in which domestic law was applied. Where a national court applies the law in an arbitrary manner, this may lead to a finding of a violation of the ECHR, most notably of Article 6.

It should also be taken into account that the Republic of Croatia, as a sovereign State, has transferred part of its judicial jurisdiction to the ECtHR and that, consequently, in proceedings concerning constitutional complaints before the Constitutional Court of the Republic of Croatia, the legal standards developed in the case law of the ECtHR are directly applicable. Furthermore, the decision of the Constitutional Court represents the final domestic decision in such proceedings, against which applicants may lodge an individual application with the ECtHR.¹⁰ In other words, this framework enables disputes to be resolved at the national level through the direct application of the ECHR and the jurisprudence of the ECtHR, in accordance with the principle of subsidiarity of the Convention supervisory system.¹¹

2. THE RIGHT OF ACCESS TO A COURT AND FINANCIAL BARRIERS UNDER THE CONVENTION

Although Article 6 of the ECHR does not explicitly refer to a right of access to a court, but rather guarantees the "right to a tribunal" in paragraph 1, the ECtHR has derived the right of access to a court as a necessary precondition for the effective enjoyment of all other procedural guarantees under Article 6. It is evident that the objective of a public, prompt and fair hearing cannot be achieved if proceedings are not initiated at all. The provision encompasses both civil and criminal aspects.¹² However, the ECtHR frequently does not draw a strict distinction between these two categories of proceedings and, in criminal matters, often relies

¹⁰ Šarin, D.; Šeparović, V., *The Constitutional Complaint as a Specific (Subsidiary) Remedy for the Protection of Human Rights and Fundamental Freedoms*, FIP – Financije i pravo, Vol. 9, No. 1/2021, pp. 21–52, p. 24.

¹¹ On the principles and doctrines developed in the case law of the ECtHR (effectiveness, autonomous interpretation, evolutionary interpretation, subsidiarity, proportionality, margin of appreciation, prohibition of abuse of rights, legal certainty, positive obligations and the 'fourth instance' doctrine), see: Šago, D.; Vukušić, I., *Organizacija pravosuđa*, Pravni fakultet Sveučilišta u Splitu, Split 2021., pp. 425–435; Marochini Zrinski, M., *Challenges in the Application and Interpretation of the Convention in the Republic of Croatia*, Zbornik radova Pravnog fakulteta u Splitu, Vol. 55, No. 2/2018, pp. 423–446.

¹² Grdinić, E., *The General Guarantee of a Fair Trial in Criminal Proceedings and the Presumption of Innocence under Article 6 §§ 1 and 2 of the Convention*, Hrvatska pravna revija, Vol. 6, No. 1/2006, pp. 7–17.

on interpretations developed in cases concerning civil rights and obligations.¹³ The right to a court is guaranteed in all cases involving the determination of civil rights and obligations, regardless of whether the claims arise from private-law relationships or concern disputes between individuals and the State or public authorities.¹⁴

Nevertheless, Contracting States are entitled to impose certain limitations on the right of access to a court. Such limitations must pursue a legitimate aim, be proportionate to that aim, and must not impair the very essence of the right.¹⁵ In numerous judgments, the ECtHR has emphasised that it is not its role to substitute itself for domestic courts, since it is for national authorities and courts to interpret and apply domestic legislation. The ECtHR's task is to determine whether the effects of such interpretation are compatible with the ECHR, particularly with regard to the application of procedural rules by domestic courts. The ECtHR is not called upon to assess whether the legal system of a Contracting State is designed in the most favourable manner for an applicant. Rather, its role is to determine whether the applicant's right of access to a court has been restricted in a disproportionate manner.¹⁶

The ECtHR has also held that the right of access to a court must be interpreted as encompassing the possibility for a party to be represented by a lawyer capable of effectively defending his or her rights. In this context, the Court delivered a judgment in a case in which the applicant was in a precarious financial situation and the divorce proceedings in question were particularly complex.¹⁷ Although the applicant was not formally required to be represented by a lawyer and was not entitled to legal aid, the ECtHR concluded that, without professional legal assistance, she had no realistic prospect of success in the proceedings and that her right of access to a court had therefore been violated. While the text of the ECHR explicitly guarantees free legal assistance only in criminal matters, the Court thus extended its protection to civil proceedings where the lack of legal aid substantially impaired the applicant's ability to effectively defend his or her rights

¹³ Šarin, D., *Preconditions for Access to a Court – Legal Positions and Case Law of the European Court of Human Rights*, Pravni vjesnik, Vol. 32, No. 1/2016, pp. 95–120; Elijaš, D.; Marković, S.; Trgovac, S., *The Right of Access to a Court as an Aspect of the Right to a Fair Trial*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, Vol. 37, No. 1/2016, pp. 385–421; Lovrić, M., *The Right of Access to a Court as the Essence of the Rule of Law*, FIP – Financije i pravo, Vol. 7, No. 1/2019, pp. 31–63.

¹⁴ Uzelac, A., *op. cit.* in fn. 9, p. 107.

¹⁵ See, for example: Marković and Others v. Italy, no. 1398/03, judgment of 14 December 2006; Tolstoy Miloslavsky v. the United Kingdom, no. 18139/91, judgment of 13 July 1995.

¹⁶ Šarin, D., *op. cit.* in fn. 13, p. 102.

¹⁷ Airey v. Ireland, no. 6289/73, judgment of 9 October 1979.

and interests. A similar issue arises in relation to court fees and litigation costs, which—particularly in light of their increasing levels—may likewise result in a violation of the right of access to a court.

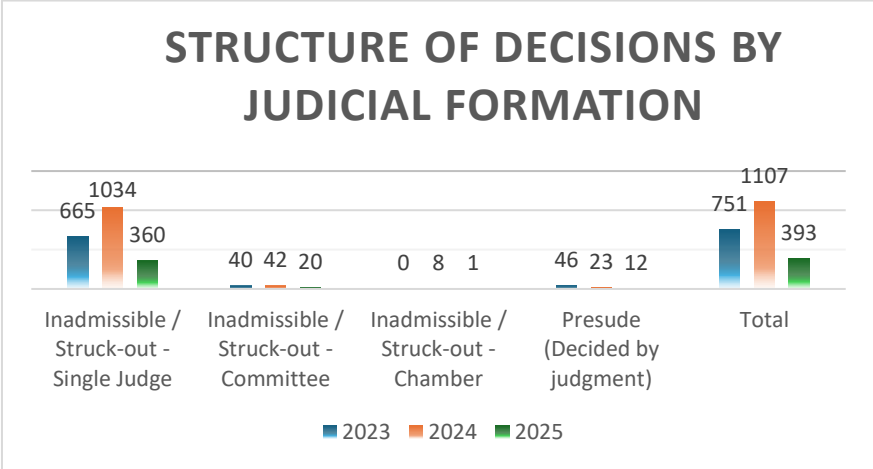
In response to the high number of violations of Article 6 of the ECHR in Croatia, the State has, over the past two decades, initiated a series of legislative reforms aimed at reducing infringements of the right of access to a court. A significant part of these reforms involved transferring certain matters from the sphere of administrative proceedings and administrative adjudication into the jurisdiction of the courts.¹⁸ However, the fact that the ECHR refers to an “independent and impartial tribunal” does not necessarily mean that all elements of a fair trial could not be ensured within administrative procedures. Unfortunately, instead of addressing the more fundamental issue, namely, the qualitative improvement of administrative proceedings, greater emphasis was placed on formal restructuring, particularly on increasing the number of cases falling within judicial jurisdiction. This approach risks creating a vicious circle: expanding judicial competence inevitably increases the caseload of judges, thereby potentially jeopardising another essential component of Article 6 of the ECHR, namely the right to a hearing within a reasonable time.

2.3. Applications against the Republic of Croatia before the ECtHR – A Statistical Overview

In this part of the paper, official statistical data of the ECtHR are used, encompassing all decisions on admissibility and merits delivered in the observed years. According to the available data from the European Court of Human Rights – Country Profile: Croatia, in 2023 the ECtHR decided on 751 applications lodged against the Republic of Croatia. Of that number, 665 applications were declared inadmissible or struck out by a Single Judge, 40 applications were decided by a three-judge Committee, while 46 cases were resolved by judgment.¹⁹

¹⁸ Legislative amendments concerned, *inter alia*, expropriation proceedings, certain status issues in family law, and proceedings concerning persons with mental disabilities.

¹⁹ European Court of Human Rights, Country Profile: Croatia, pp. 1–2, available at: https://www.echr.coe.int/d/cp_croatia_eng, accessed 10 January 2026.



Graph No. 1.²⁰

In 2024, the ECtHR dealt with 1,107 applications, of which 1,084 were declared inadmissible or struck out of the list of cases, while 22 judgments were delivered concerning 23 applications; in 21 of those cases, the ECtHR found at least one violation of the ECHR. In the period from January to July 2025, the ECtHR processed 393 applications, of which 360 were declared inadmissible by a Single Judge, 20 by a three-judge Committee, and 1 by a seven-judge Chamber, while 12 applications were resolved by judgment.²¹

Such statistical indicators suggest that the majority of applications against Croatia do not pass the admissibility threshold, meaning that a significant number of cases are resolved already at the initial stage of the proceedings.

2.3.1. Overview of Pending Cases

According to the most recent available data of the ECtHR, the total number of pending cases against the Republic of Croatia as of 1 July 2025 amounts to 558. The structure of these cases according to judicial formation, as previously described, is presented in Table 1.²²

²⁰ Data for 2025 refer to the period from January to July 2025.

²¹ European Court of Human Rights, Country Profile: Croatia, p. 1, available at: https://www.echr.coe.int/d/cp_croatia_eng, accessed 10 August 2025.

²² Table 1 presents the structure of pending cases according to judicial formation, status as of 1 July 2025.

Composition of the Court	Number	Percentage
<i>Single Judge</i> (1 judge)	350	62,72%
<i>Committee</i> (3 judges)	165	29,57%
<i>Chamber</i> (7 judges)	43	7,71%
<i>Grand Chamber</i> (17 judges)	0	0,00%
Total Pending	558	100,00%

Table. 1.

The table shows that the largest number of cases - 350 cases, or 62.72% of the total - falls within the jurisdiction of a Single Judge. This figure is particularly significant, as a Single Judge typically decides applications that are considered manifestly inadmissible or that fail to meet the basic procedural requirements for examination before the Court.

A three-judge Committee is currently dealing with 165 cases, representing 29.57% of the total number of pending applications. This formation examines more complex cases that require preliminary consideration by more than one judge.

A seven-judge Chamber, which constitutes the ordinary judicial formation for determining cases on the merits, is currently dealing with 43 cases (7.71%). These cases usually involve serious allegations of violations of the ECHR that warrant detailed examination.

The Grand Chamber, which represents the highest judicial formation of the ECtHR, currently has no pending cases against Croatia (0.00%). The distribution of pending cases clearly indicates that a substantial majority of applications against Croatia do not satisfy the fundamental procedural requirements for examination before the Court. The fact that 62.72% of cases fall within the competence of a Single Judge may point either to insufficient legal awareness of admissibility criteria on the part of applicants or to the frequent submission of applications that do not meet the procedural requirements laid down by the ECHR.

2.3.2. Analysis by Type of Convention Violation

An analysis of ECtHR judgments according to the provisions of the ECHR represents a key indicator of the areas in which the Republic of Croatia most frequently fails to meet human rights protection standards. Based on a review of all relevant judgments available in the publicly accessible data of the Court, a total of 40 cases were identified in which a merits decision was delivered concerning alleged violations of the ECHR. The analysis is limited to judgments in which the ECtHR ruled on the merits of the alleged violations.

CONVENTION PROVISION	Violation found	No violation found	Total	Percentage of total
Article 6 – Right to a fair trial	6	7	13	32,50%
Article 3 – Prohibition of torture and inhuman or degrading treatment	2	3	5	12,50%
Article 14 – Prohibition of discrimination	4	1	5	12,50%
Article 1 of Protocol No. 1 – Protection of property	3	2	5	12,50%
Article 5 – Right to liberty and security	1	1	2	5,00%
Article 8 – Right to respect for private and family life	1	1	2	5,00%
Article 10 – Freedom of expression	1	1	2	5,00%
Article 4 – Prohibition of slavery and forced labour	1	0	1	2,50%
Article 2 – Right to life	1	0	1	2,50%
Article 9 – Freedom of thought, conscience and religion	1	0	1	2,50%
Article 11 – Freedom of assembly and association	1	0	1	2,50%
Article 7 – No punishment without law	0	1	1	2,50%
Article 4 of Protocol No. 7 – Right not to be tried or punished twice	0	1	1	2,50%
TOTAL	22	18	40	100,00%

Table No. 2.

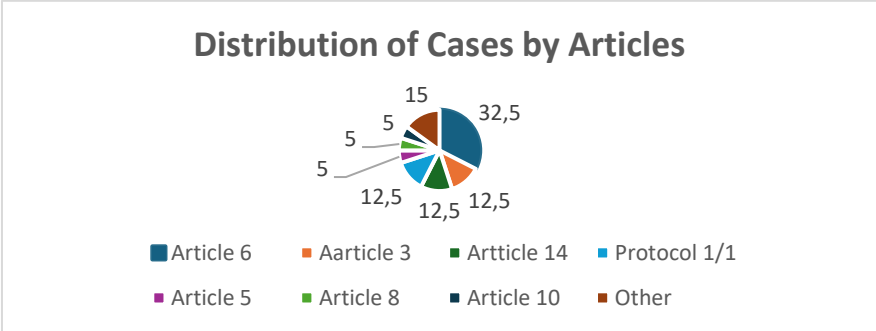


Figure. 1.

The data clearly show that Article 6 of the ECHR, concerning the right to a fair trial, accounts for 32.50% of all such cases. This indicates that issues related to the fairness of judicial proceedings constitute the most problematic area within the Croatian legal system.

Overall, in 22 cases (55.00%) the ECtHR found at least one violation of the ECHR, whereas in 18 cases (45.00%) it concluded that no violation had occurred. A violation rate of 55% in cases that reach a merits decision is significant and calls for particular attention on the part of national authorities.²³

SUBCATEGORY	Violation found	No violation found	Violation rate
Right to a fair trial within a reasonable time	3	2	60,00%
Access to a court	1	1	50,00%
Right to legal assistance of one’s own choosing	1	1	50,00%
Impartiality of the court	0	1	0,00%
Presumption of innocence	1	0	100,00%
Other defence rights guarantees	0	2	0,00%
TOTAL	6	7	46,15%

Table No. 2.

Thus, Article 6 of the ECHR represents by far the most frequently invoked provision in cases against the Republic of Croatia, encompassing nearly one third of all cases decided on the merits.

²³ Due to the small number of analysed cases within certain subcategories, the calculated violation rates have limited statistical representativeness.

The following section presents the success rate of applications according to individual Articles of the ECHR.

RANK	Article	Success rate	Total number of cases
1.	Articles 2., 4., 9., 11.	100,00%	4 (1 each)
2.	Article 14.	80,00%	5
3.	Protocol 1/1	60,00%	5
4.	Articles 5., 8., 10.	50,00%	6 (2 each)
5.	Article 6.	46,15%	13
6.	Article 3.	40,00%	5
7.	Article 7., Protocol 7/4	0,00%	2 (1 each)

Table 4.

Articles 2, 4, 9 and 11 show a success rate of 100%; however, the number of cases is very small (one each), which does not allow for firm general conclusions. Article 14, concerning the prohibition of discrimination, demonstrates a high success rate of 80%, suggesting that when discrimination cases reach the Court, there is a strong likelihood of a finding of a violation. This may point to serious systemic shortcomings in the protection of vulnerable groups in Croatia. Article 6, although the most frequently invoked provision, shows a comparatively lower success rate (46.15%), indicating that the ECtHR rigorously assesses allegations of violations of the right to a fair trial and does not automatically find violations in all such cases.

3. COSTS BEFORE THE ECtHR

Proceedings before the ECtHR are designed as a mechanism of international protection of fundamental rights which must be genuinely and effectively accessible to individuals.²⁴ In accordance with the principle of effectiveness of the Convention system, access to the Court must not be prevented or disproportionately hindered by financial obstacles.²⁵

In this regard, proceedings before the ECtHR are, as a rule, free of charge: no court fees are payable for the lodging of an individual application, and legal

²⁴ See Article 34 of the Convention.

²⁵ *Loizidou v. Turkey*, no. 15318/89, judgment of 18 December 1996, available at: <https://hudoc.echr.coe.int/eng?i=001-45610>, accessed 12 January 2026.

representation is not mandatory at the initial stage of the proceedings.²⁶ Such an arrangement constitutes a direct consequence of the right of individual application guaranteed by Article 34 of the ECHR and confirms the understanding that access to the Court represents one of the fundamental guarantees of the effectiveness of the human rights protection system.²⁷

Although legal representation is not obligatory before the ECtHR notifies the respondent State of the application (notification), its importance increases as the proceedings advance.²⁸ The Rules of Court²⁹ provide that, once the respondent Government has been notified of the application, the applicant must, as a rule, be represented by a lawyer authorised to practise in one of the Contracting States, in accordance with Rule 36 of the Rules of Court. This requirement ensures the professional conduct of the proceedings at stages involving the examination of admissibility and the merits, as well as in the phase concerning just satisfaction, including costs and expenses.³⁰

The legal basis for awarding costs and expenses before the ECtHR is set out in Article 41 of the ECHR, which empowers the Court, where it finds a violation of the ECHR, to afford just satisfaction to the injured party. Within this framework, the ECtHR may also award reimbursement of costs and expenses incurred by the applicant in the proceedings before domestic authorities and before the Court itself.³¹ However, the award of costs is not an automatic consequence of a finding of a violation; rather, it depends on the Court's discretionary assessment in each individual case as to whether the relevant conditions have been satisfied.³²

²⁶ Rules of Court of the European Court of Human Rights, Chapter I – General Provisions on Proceedings.

²⁷ *Mamatkulov and Askarov v. Turkey*, nos. 46827/99 and 46951/99, judgment of 4 February 2005, available at: <https://hudoc.echr.coe.int/?i=001-68183>, accessed 13 January 2026.

²⁸ Rules of Court, Rule 36 (Representation of Applicants).

²⁹ Rules of Court of the European Court of Human Rights, available at: <https://uredzastupnika.gov.hr/UserDocsImages/dokumenti/POSLOVNIK/Poslovnik%20E%20SLJPa.pdf>, accessed 16 January 2026 (hereinafter: Rules of Court).

³⁰ European Court of Human Rights, Practice Direction – Just Satisfaction Claims, available at: https://www.echr.coe.int/documents/d/echr/PD_satisfaction_claims_ENG, accessed 13 January 2026, Sections I–III.

³¹ *Ibid.*, Section II.

³² In accordance with the Rules of Court and the practice relating to just satisfaction, the Court awards compensation only insofar as it considers it equitable in the circumstances of the case. The Court may find that the mere finding of a violation constitutes sufficient just satisfaction. It may also award a lower sum than that actually claimed or decide not to award any compensation.

These conditions are elaborated in detail in the Rules of Court, in particular Rule 60, as well as in the Court's Practice Direction on Just Satisfaction Claims.³³ According to the Court's established case law, costs and expenses may be awarded only insofar as they were actually incurred, were necessary to prevent or redress the violation of the ECHR, and are reasonable as to quantum. In this respect, the ECtHR retains a wide margin of appreciation in assessing the proportionality of the sums claimed, taking into account the complexity of the case, the extent of the legal work performed and the outcome of the proceedings.³⁴

In practice, this means that the ECtHR frequently reduces excessive claims, even where it accepts that the applicant is entitled to reimbursement of costs.³⁵ In particular, the Court rejects claims that are not adequately supported by documentary evidence, are not sufficiently itemised, or relate to complaints that did not lead to a finding of a violation or were declared inadmissible. The burden of proving the existence, necessity and reasonableness of the claimed costs rests with the applicant.

From the total amount claimed, any sums already covered by domestic legal aid or by legal aid granted within the ECtHR system are deducted in order to prevent double recovery of the same expenses.³⁶ The Rules of Court expressly provide that a judgment must, where appropriate, contain a decision concerning the costs of the proceedings. This ensures that the issue of costs and expenses forms an integral part of the judicial decision and is determined within the operative provisions of the judgment, in accordance with the rules governing just satisfaction and the Court's discretionary assessment in the specific case.³⁷

With regard to the costs of the participation of witnesses, experts and other persons before a delegation, the Rules of Court provide that the costs of their attendance shall, as a rule, be borne by the party at whose request or on whose behalf they were summoned, unless the Chamber decides otherwise. In other cases, the Chamber determines whether the costs shall be borne by the Council of Europe or

³³ European Court of Human Rights, Practice Direction – Just Satisfaction Claims, available at: https://www.echr.coe.int/documents/d/echr/PD_satisfaction_claims_HRV, accessed 18 January 2026.

³⁴ Rules of Court, Part III – Just Satisfaction Claims, section on material conditions: costs and expenses.

³⁵ See: *Tomašić v. Croatia*, no. 21753/03, judgment of 19 October 2006, available at: <https://www.iusinfo.hr/sudska-praksa/ECHR701Y1995N18139S91U001M57947>, accessed 15 January 2026.

³⁶ Rules of Court, provisions on legal aid.

³⁷ Rules of Court, Rule 74 § 1 (j).

awarded against the applicant or a third party, the amount of such costs being fixed by the President of the Chamber.³⁸

In the event of a friendly settlement or a unilateral declaration by the respondent State, the issue of costs may be regulated within the framework of such a settlement, in accordance with Article 39 of the ECHR. Furthermore, where an application is struck out of the list of cases pursuant to Article 37 of the ECHR (strike-out), the ECtHR retains discretion to decide on costs in the strike-out decision itself, in accordance with Rule 43 § 4 of the Rules of Court.

The Rules of Court also establish a specific system of legal aid intended to ensure effective access to the Court for applicants who lack sufficient financial means. The President of the Chamber may, either upon request by the applicant or of his or her own motion, grant legal aid for representation before the Court after the respondent Contracting Party has submitted written observations on the admissibility of the application or after the expiry of the time-limit for such submission. Subject to the fulfilment of the prescribed conditions, legal aid granted at this stage also applies to proceedings before the Grand Chamber.³⁹

Legal aid may be granted only if the President of the Chamber considers that it is necessary for the proper conduct of the proceedings and that the applicant lacks sufficient financial resources to meet all or part of the costs of the proceedings.⁴⁰ For the purpose of assessing the applicant's financial situation, the applicant is required to submit a certified declaration of income, assets and financial obligations, while the President of the Chamber may also request observations from the respondent Contracting Party. The parties are notified of the decision on legal aid through the Registry of the Court.⁴¹

The scope of legal aid covers not only the fees of the lawyer or other appointed representative but also other necessary expenses, including travel expenses, subsistence allowances and similar costs incurred in connection with the proceedings before the Court. The amounts payable under the legal aid scheme are determined by the Registrar of the Court in accordance with the applicable scales.⁴²

³⁸ Rules of Court, Rule A5 § 6.

³⁹ Rules of Court, Chapter XII – Legal Aid, Rule 105.

⁴⁰ Rules of Court, Rule 106.

⁴¹ Rules of Court, Rule 107.

⁴² Rules of Court, Rules 108–109.

A decision granting legal aid is not final in nature; the President of the Chamber retains the authority to modify or withdraw it at any time if it is established that the conditions for its grant are no longer satisfied.⁴³

4. COSTS OF PROCEEDINGS BEFORE THE CONSTITUTIONAL COURT OF THE REPUBLIC OF CROATIA

The costs of proceedings before the Constitutional Court of the Republic of Croatia encompass a wide range of expenses arising in the course of constitutional adjudication, including the operational costs of the Court, costs of expert opinions, translation expenses, travel costs of participants, and, in particular, costs of legal representation by attorneys.

The normative regulation of these costs is contained in Article 23 of the Constitutional Act on the Constitutional Court of the Republic of Croatia⁴⁴, according to which each participant shall, as a rule, bear his or her own costs, unless the Constitutional Court decides otherwise.

Such a legislative solution aims to prevent the overburdening of the Constitutional Court with unfounded complaints while simultaneously protecting the State budget. However, in practice, the mechanical and formalistic application of this provision has proven capable of producing disproportionate consequences for individuals.

For many years, the Constitutional Court's practice consisted of routinely rejecting requests for reimbursement of costs of constitutional complaint proceedings by means of a summary reference to Article 23 of the Constitutional Act, without providing individualised reasoning in each specific case.

This approach proved controversial, particularly after the application of the aforementioned provision was examined in the case of *Dragan Kovačević v. Croatia*⁴⁵ before the ECtHR, in which the Court concluded that the refusal to reimburse the costs of a constitutional complaint, despite the applicant's success,

⁴³ Rules of Court, Rule 110.

⁴⁴ Constitutional Act on the Constitutional Court of the Republic of Croatia, Official Gazette Nos. 99/99, 29/02, 49/02.

⁴⁵ *Dragan Kovačević v. Croatia*, no. 49281/15, judgment of 12 May 2022, available at: <https://hudoc.echr.coe.int/eng?i=001-217418>, accessed 15 January 2026.

constituted a violation of the right of access to a court guaranteed by Article 6 § 1 of the European Convention on Human Rights.⁴⁶

Although, in decision no. U-III-1380/2014 of 20 May 2015⁴⁷, the Constitutional Court upheld the constitutional complaint and quashed the decisions of the ordinary courts by which the applicant had been completely deprived of legal capacity, it confined itself, with regard to costs, to a literal reiteration of the wording of Article 23 of the Constitutional Act, without explaining why it had not applied the exception provided for in that provision. According to the ECtHR, this resulted in the imposition of a disproportionate financial burden on the applicant, particularly given that his legal costs amounted to EUR 815, whereas his monthly income from disability benefits was only EUR 164.

The ECtHR emphasised that legal representation before the Constitutional Court cannot be regarded as unnecessary or excessive, since that court decides on complex legal issues that are often incomprehensible to laypersons; accordingly, the engagement of professional legal assistance must be viewed not merely as justified but as necessary.⁴⁸ The Court further stressed that the proceedings in question had status-related and existential consequences for the applicant, as the ordinary courts had ruled on his legal capacity, thereby reinforcing the necessity of professional representation. The financial burden, although calculated in accordance with the Bar Tariff on Attorneys' Fees and Reimbursement of Expenses⁴⁹, was manifestly disproportionate to the applicant's income and impaired the very essence of his right of access to a court.

In its proportionality assessment, the ECtHR also relied on its earlier case law, in particular Černius and Rinkevičius v. Lithuania⁵⁰, in which it was held that

⁴⁶ Act on the Ratification of the Convention for the Protection of Human Rights and Fundamental Freedoms and Protocols Nos. 1, 4, 6, 7 and 11 thereto (Official Gazette, No. 18/1997).

⁴⁷ Constitutional Court of the Republic of Croatia, decision no. U-III-1380/2014 of 20 May 2015. In that decision, the Constitutional Court upheld the constitutional complaint and quashed the decisions of the Bjelovar County Court (no. Gž-1279/2013-2 of 23 January 2014) and the Slatina Municipal Court (no. R1-74/12-14 of 5 March 2013), by which the applicant had been fully deprived of legal capacity. In his constitutional complaint, the applicant alleged violations of Articles 14, 29, 35 and 57 § 1 of the Constitution, as well as Articles 6 and 8 of the Convention and Article 12 of the UN Convention on the Rights of Persons with Disabilities.

⁴⁸ Dragan Kovačević v. Croatia, §§ 56–60.

⁴⁹ Tariff on Attorneys' Fees and Reimbursement of Costs (Official Gazette Nos. 142/12, 103/14, 118/14, 107/15, 37/22).

⁵⁰ Černius and Rinkevičius v. Lithuania, nos. 73579/17 and 14620/18, judgment of 18 June 2020.

national courts must conduct a proportionality test between the financial burden imposed and the benefit obtained by the applicant through success in the proceedings. If such a test is disregarded, a situation may arise in which a party, despite prevailing in the proceedings, remains in a financially worse position than before initiating them, thereby undermining the very purpose of judicial protection.⁵¹

In the Croatian context, additional weight was attached to the fact that domestic legislation does not provide for the possibility of free legal aid in proceedings before the Constitutional Court, which, combined with the rigid application of Article 23 of the Constitutional Act, resulted in a disproportionate restriction of the applicant's right of access to a court.

Ultimately, the ECtHR concluded that the formally legitimate aims underlying Article 23 of the Constitutional Act, such as preventing the overburdening of the Constitutional Court and protecting the State budget, could not, in the specific circumstances of the case, be regarded as proportionately pursued. The Constitutional Court had failed to provide relevant and sufficient reasons for refusing to award costs, limiting itself to a literal citation of the statutory provision. Such an approach did not satisfy the standard of reasoning required of judicial decisions, nor did it ensure a fair balance between legitimate aims and the protection of individual rights. Consequently, the ECtHR found a violation of Article 6 § 1 of the Convention.

In response to that judgment, the Constitutional Court, in decision no. U-III-3686/2019 of 20 December 2022⁵², modified its previous practice and established new principles concerning the reimbursement of costs in constitutional complaint proceedings. The Court stated that, in exercising its discretionary power under Article 23 of the Constitutional Act, it would henceforth assess requests for costs on the basis of criteria such as the nature of the proceedings, the importance of the case for the applicant, the personal vulnerability of the party concerned, and whether the obligation to bear costs would constitute an excessive financial burden. In order to enable such an assessment, applicants are required to substantiate their claims, provide detailed information on the financial situation of their household, and submit appropriate documentation.⁵³

⁵¹ *Bibić v. Croatia*, judgment of 13 April 2000; see also *Pham Hoang v. France*, judgment of 25 September 1992, § 40.

⁵² Constitutional Court of the Republic of Croatia, decision no. U-III-3686/2019 of 20 December 2022 (Official Gazette, No. 5/23), including dissenting opinions.

⁵³ *Ibid.*, para. 44.

The case U-III-3686/2019 concerned a constitutional complaint lodged by Dražen Švarc, who challenged decisions of the ordinary courts delivered in civil proceedings concerning the establishment of liability and the award of damages. After the Constitutional Court upheld the complaint and found a violation of the applicant's rights, the issue arose as to the reimbursement of the costs of the constitutional proceedings, in particular the costs of drafting the constitutional complaint. The applicant emphasised that he had incurred substantial representation costs and that the failure to reimburse them, despite his success in the proceedings, would constitute an excessive financial burden.

In that case, the Constitutional Court explicitly confronted, for the first time, arguments which it had regularly dismissed in its earlier practice—almost invariably relying solely on Article 23 of the Constitutional Act, according to which each participant bears his or her own costs unless the Court decides otherwise. For many years, requests for reimbursement of costs had been rejected routinely, without an individualised assessment of the importance of the case, the applicant's financial situation, or the significance of the constitutional complaint itself.

Decision U-III-3686/2019 is therefore rightly regarded as a "leading" decision, as it established for the first time a structured set of criteria for deciding on the costs of constitutional complaint proceedings. In doing so, the Constitutional Court not only responded to the requirements formulated by the ECtHR in *Kovačević*, but also enhanced the predictability of domestic practice and aligned it more closely with the standards of Article 6 of the ECHR.

Prior to the shift in constitutional practice following the judgment in *Kovačević*, the ECtHR had already addressed the issue of costs of constitutional proceedings in the context of a family-law dispute in *Moskalj v. Croatia*⁵⁴. Following her divorce and a judgment awarding custody of her minor son to her, the applicant initiated enforcement proceedings in order to secure the execution of that decision. However, the enforcement proceedings and other legal remedies proved protracted and ineffective, ultimately resulting in the child continuing to live with the father despite the final judgment.⁵⁵

Due to the inefficiency and excessive length of the proceedings, the applicant lodged a constitutional complaint alleging a violation of her right to a hearing within a reasonable time (Article 29 § 1 of the Constitution of the Republic of

⁵⁴ *Moskalj v. Croatia*, no. 60272/21, judgment of 15 October 2024.

⁵⁵ *Ibid.*, §§ 6–15.

Croatia) and her right to respect for family life (Article 35 of the Constitution; Article 8 of the ECHR). On 15 December 2021, the Constitutional Court partially upheld the complaint, finding the alleged violations and awarding her HRK 5,000 (EUR 663.61) in respect of non-pecuniary damage.⁵⁶ At the same time, however, it rejected her claim for reimbursement of the costs of the constitutional proceedings, amounting to HRK 6,125 (EUR 812.93), relying on Article 23 of the Constitutional Act and stating that there were no grounds in the specific circumstances to depart from the general rule that each party bears its own costs. The applicant subsequently lodged an application with the ECtHR, arguing that the refusal to reimburse her costs, despite the partial success of her constitutional complaint, violated her right of access to a court under Article 6 § 1 of the ECHR. In its judgment, the Court referred to its previous case law, in particular *Bibić v. Croatia* and *Kovačević v. Croatia*, emphasising that proceedings before the Constitutional Court involve complex legal issues and that legal assistance by a lawyer in such proceedings constitutes a necessity rather than a luxury.⁵⁷ The Court further stressed that, in deciding on costs, national courts must take into account the applicant's financial situation and the proportionality of the financial burden imposed; otherwise, the right of access to a court may become illusory.

In the specific circumstances of the case, the ECtHR found that the applicant, although formally successful, had been placed in a worse financial position than before initiating the proceedings: the cost of the constitutional complaint (EUR 813) exceeded the compensation awarded by the Constitutional Court (EUR 664). Moreover, the Constitutional Court had confined itself to a mere reference to Article 23 of the Constitutional Act, without providing relevant and sufficient reasons. The ECtHR considered such an approach incompatible with the Convention, as it failed to satisfy the requirement of adequate reasoning in judicial decisions.⁵⁸

Accordingly, the ECtHR unanimously found a violation of Article 6 § 1 of the ECHR and awarded the applicant just satisfaction: EUR 1,016 in respect of pecuniary damage (including the costs of the constitutional complaint and other domestic remedies), EUR 865 for the costs and expenses incurred before the ECtHR, and EUR 3,000 in respect of non-pecuniary damage.⁵⁹

⁵⁶ Constitutional Court of the Republic of Croatia, decision of 15 December 2021 (as cited in *Moskalj v. Croatia*).

⁵⁷ *Bibić v. Croatia*, judgment of 13 April 2000, no. 1620/10; see also *Dragan Kovačević v. Croatia*, no. 49281/15, judgment of 12 May 2022.

⁵⁸ *Moskalj v. Croatia*, §§ 56–60.

⁵⁹ *Ibid.*

The Moskalj judgment thus further confirmed the obligation of the Republic of Croatia, pursuant to Article 46 of the ECHR, to ensure a change in the practice of the Constitutional Court so as to prevent situations in which applicants, despite succeeding before the Constitutional Court, are left to bear a disproportionate financial burden.

4.1. The Impact of the ECtHR Case Law on the Practice of the Constitutional Court

Following the judgment of the ECtHR in Dragan Kovačević v. Croatia, the recent practice of the Constitutional Court demonstrates a gradual departure from a strictly formalistic approach to Article 23 of the Constitutional Act and the adoption of a more flexible interpretation requiring an individualised proportionality assessment in each specific case.⁶⁰ The most significant example of this shift is decision no. U-III-5169/2019, in which the Constitutional Court awarded the applicant reimbursement of the costs of constitutional complaint proceedings in the amount of EUR 830.00, marking the first clear departure from its previous restrictive practice.⁶¹

The factual background of the case reveals the complexity of the circumstances in which this decision was rendered. The applicant, who had been serving a long-term prison sentence in Lepoglava Penitentiary since 2011, lodged a constitutional complaint through legal counsel on 18 January 2019.⁶² In his complaint, he alleged violations of fundamental constitutional rights—the right to liberty and personal security (Article 23 § 1 of the Constitution), the right to dignity and humane treatment (Article 25 § 1), the right to a fair trial (Article 29 § 1), and the right to respect for private and family life (Article 35)—as well as violations of rights guaranteed under the ECHR (Articles 3, 6 § 1 and 8). He also sought reimbursement of the costs of drafting the constitutional complaint in the amount of HRK 5,000 (EUR 664), plus value-added tax.

On 15 January 2025, the Constitutional Court partially upheld the complaint in the part relating to the applicant's conditions of detention and hygiene during his stay

⁶⁰ See *supra*.

⁶¹ Constitutional Court of the Republic of Croatia, decision no. U-III-5169/2019 of 11 March 2025.

⁶² Graovac, G.; Gregori, G., *Jurisdiction of the Constitutional Court of the Republic of Croatia ratione materiae concerning constitutional complaints related to pre-trial detention*, Croatian Annual of Criminal Law and Practice, Vol. 24, No. 1/2017, pp. 117–140.

in Zagreb Prison, finding that the rights deriving from human dignity and Article 3 of the ECHR had been violated. However, it did not decide at that stage on the request for reimbursement of costs, expressly stating that this issue would be addressed subsequently. Only after an additional procedural step, in which the applicant was requested on 15 June 2023 to specify and document his claim, was the Court able to rule on the costs. In his reply of 25 July 2023, the applicant stated that he had been deprived of liberty for almost twelve years, had no income whatsoever, and submitted a certificate from the Ministry of Justice confirming this fact.

The Constitutional Court subsequently established that, at an earlier stage, the applicant had exhausted all available legal mechanisms—a request for judicial protection under Article 17 of the Execution of Prison Sentences Act⁶³ had remained unresolved, an attempt to reach an amicable settlement with the State Attorney's Office had failed, and a civil action for non-pecuniary damage before the ordinary courts had not provided effective protection. Since only the constitutional complaint had ultimately enabled the protection of his rights, the Court considered that the proceedings were of status-related and existential importance, in which professional legal assistance was necessary.

In deciding on costs, the Constitutional Court relied on the principles set out in decision U-III-3686/2019, emphasising that it was necessary to assess whether the obligation to bear costs would impose an excessive burden on the applicant.⁶⁴ Given that the amount of HRK 5,000 (EUR 664), plus VAT, represented an insurmountable obstacle for a person without any income, the Court concluded that a strict application of Article 23 of the Constitutional Act would, in this case, be incompatible with the principle of fairness. Taking into account European standards and the obligation of the Republic of Croatia under Article 46 of the ECHR⁶⁵ to align its practice with the judgments of the ECtHR, the Constitutional Court awarded reimbursement of costs in the amount of EUR 830.00, to be paid from the State budget.

Decision U-III-5169/2019 constitutes a turning point in constitutional practice, as it confirms that the purpose of Article 23 of the Constitutional Act is not absolute and does not permit mechanical application, but rather includes an exception allowing flexibility where required by the protection of individual rights. Through

⁶³ Enforcement of Prison Sentence Act (Official Gazette Nos. 14/21, 155/23).

⁶⁴ Constitutional Court of the Republic of Croatia, decision no. U-III-3686/2019 of 20 December 2022, §§ 40–50.

⁶⁵ See Article 46 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

this approach, the Constitutional Court clearly affirmed that the objective is to strike a balance between preventing abuse of the constitutional complaint mechanism and safeguarding the State budget, on the one hand, and ensuring an effective right of access to a court, on the other.⁶⁶

Furthermore, in decision no. U-III-2883/2018 of 2 March 2023, the Constitutional Court upheld the constitutional complaint of a detainee who had alleged inhuman conditions in Zagreb Prison, quashed the judgments of the Karlovac County Court and the Zagreb Municipal Civil Court, and remitted the case for fresh examination.⁶⁷ The applicant had been held between 24 February 2011 and 19 January 2012 in overcrowded prison cells with insufficient personal space and inadequate sanitary conditions, which the Constitutional Court found to constitute a violation of Article 3 of the ECHR and Articles 23 and 25 of the Constitution. In doing so, the Court applied ECtHR standards concerning minimum personal space in detention facilities—holding that space below three square metres per detainee gives rise to a strong presumption of a violation of Article 3, whereas space between three and four square metres requires a strict proportionality assessment.⁶⁸ The Court further pointed to inconsistencies in the second-instance judgment, particularly the absence of a factual basis in the case file and the disregard of relevant ECtHR case law on just satisfaction.

The case is also of particular importance with regard to the costs of constitutional proceedings. Although the applicant's request for costs had initially not been substantiated, the Constitutional Court, in light of the standards established in *Dragan Kovačević v. Croatia*, requested additional information concerning his financial situation. It was established that the applicant's three-member household had a monthly income of approximately EUR 831, which was considered insufficient to cover the costs of legal representation without imposing an excessive financial burden. On the basis of the criteria set out in decision U-III-3686/2019 (nature and importance of the proceedings, vulnerability of the applicant, and financial burden), the Court awarded reimbursement of the costs of drafting the constitutional complaint in the amount of EUR 830.01, to be paid from the State budget within three months of submission of the request to the Ministry of Justice and Public Administration.⁶⁹

⁶⁶ Constitutional Court of the Republic of Croatia, decision no. U-III-5169/2019 of 11 March 2025.

⁶⁷ Arlović, M., *The Relationship between the Constitutional Court of the Republic of Croatia and the Judicial Power in the Republic of Croatia*, Collected Papers of the Faculty of Law in Split, Vol. 52, No. 2/2015, pp. 369–405.

⁶⁸ See: *Muršić v. Croatia*, no. 7334/13, judgment of 20 October 2016, §§ 136–141.

⁶⁹ Constitutional Court of the Republic of Croatia, decision no. U-III-1243/2020 of 20 December 2022.

Through this decision, the Constitutional Court further confirmed its new practice, according to which decisions on costs no longer depend on an automatic reference to Article 23 of the Constitutional Act but rather on an individualised assessment of the specific circumstances of each case in accordance with Convention standards.

This development confirms the consolidation of the new constitutional practice concerning the costs of constitutional complaint proceedings. Unlike the earlier approach, in which requests for costs were regularly dismissed without reasoning, the Court now systematically applies criteria of proportionality, vulnerability and financial burden in line with ECtHR standards. In this way, it further develops the line of case law initiated by *Dragan Kovačević v. Croatia* and continued in domestic decisions U-III-1243/2020 and U-III-2883/2018.⁷⁰

5. CONCLUSION

The right of access to a court, as an inherent component of Article 6 § 1 of the European Convention on Human Rights, constitutes one of the fundamental guarantees of effective judicial protection. While States enjoy a certain margin of appreciation in regulating procedural rules and the allocation of costs, financial barriers must not impair the very essence of that right. The jurisprudence of the ECtHR consistently emphasises that access to justice must be practical and effective, not theoretical or illusory.

In this context, the issue of costs in constitutional complaint proceedings in Croatia has revealed a structural tension between two legitimate objectives: safeguarding the State budget and preventing abusive litigation, on the one hand, and ensuring effective protection of fundamental rights, on the other. The long-standing practice of the Constitutional Court, characterised by a mechanical application of Article 23 of the Constitutional Act on the Constitutional Court, demonstrated the risks inherent in prioritising formal procedural rules over substantive fairness.

The judgments of the ECtHR in *Dragan Kovačević v. Croatia* and *Moskalj v. Croatia* marked a decisive turning point. By subjecting the domestic approach to a proportionality analysis, the Strasbourg Court clarified that even successful applicants may suffer a violation of their right of access to a court if the financial burden imposed upon them is excessive and insufficiently reasoned. The

⁷⁰ Constitutional Court of the Republic of Croatia, decisions no. U-III-1243/2020 of 20 December 2022 and no. U-III-2883/2018 of 2 March 2023.

requirement to conduct an individualised assessment of proportionality, taking into account the applicant's financial situation, the importance of the case and the necessity of legal representation, has thus become an essential Convention standard.

Recent constitutional case law demonstrates that the Constitutional Court has internalised these standards. Decisions such as U-III-3686/2019 and U-III-5169/2019 confirm a shift from formalism towards a more nuanced and rights-oriented approach. The Court now applies criteria of vulnerability, proportionality and financial burden in assessing claims for reimbursement of costs, thereby aligning domestic practice with the requirements flowing from Article 6 of the Convention and Article 46 concerning the binding force of ECtHR judgments.

The evolution of this jurisprudence illustrates the dynamic interaction between the Convention system and national constitutional adjudication. The ECtHR's case law has not merely corrected individual injustices but has prompted a structural recalibration of domestic procedural practice. In doing so, it reinforces the principle of subsidiarity, effective protection of Convention rights must first and foremost be secured at the national level.

Ultimately, the regulation of costs in constitutional proceedings cannot be viewed as a purely technical or budgetary matter. It directly affects the accessibility and credibility of constitutional justice. A system in which individuals succeed in establishing a violation of their fundamental rights but are left to bear disproportionate financial burdens risks undermining confidence in judicial protection itself. The recent shift in Croatian constitutional practice represents an important step towards ensuring that the right of access to a court remains effective in substance as well as in form.

REFERENCES

BOOK AND ARTICLES

1. Arlović, M., *Međudodnos Ustavnog suda Republike Hrvatske i sudbene vlasti u Republici Hrvatskoj*, Zbornik radova Pravnog fakulteta u Splitu, Vol. 52, No. 2/2015, pp. 369–405.
2. Elijaš, D.; Marković, S.; Trgovac, S., *Pravo na pristup sudu kao aspekt prava na pravično suđenje*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, Vol. 37, No. 1/2016, pp. 385–421.

3. Graovac, G.; Gregori, G., *Nadležnost Ustavnog suda Republike Hrvatske ratione materiae glede istražnozatvorskih ustavnih tužbi*, Hrvatski ljetopis za kaznene znanosti i praksu, Vol. 24, No. 1/2017, pp. 117–140.
4. Grdinić, E., *Opće jamstvo poštenog suđenja u kaznenim postupcima i presumpcija nedužnosti prema članku 6. stavcima 1. i 2. Konvencije za zaštitu ljudskih prava i temeljnih sloboda*, Hrvatska pravna revija, Vol. 6, No. 1/2006, pp. 7–17.
5. Lovrić, M., *Pravo na pristup sudu kao esencija vladavine prava*, FIP – Financije i pravo, Vol. 7, No. 1/2019, pp. 31–63.
6. Maričić, D., *Konvencija za zaštitu temeljnih prava i sloboda*, Novi informator, Zagreb 2012.
7. Marochini Zrinski, M., *Izazovi u primjeni i tumačenju Konvencije u Republici Hrvatskoj*, Zbornik radova Pravnog fakulteta u Splitu, Vol. 55, No. 2/2018, pp. 423–446.
8. Omejec, J., *Izvršenje presuda i odluka Europskog suda za ljudska prava*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 62, No. 5–6/2012, pp. 1915–1938.
9. Šago, D.; Vukušić, I., *Organizacija pravosuđa*, Pravni fakultet Sveučilišta u Splitu, Split 2021.
10. Šarin, D., *Pretpostavke za pristup sudu – pravna stajališta i praksa Europskog suda za ljudska prava*, Pravni vjesnik, Vol. 32, No. 1/2016, pp. 95–120.
11. Šarin, D.; Šeparović, V., *Ustavna tužba kao posebno (supsidijarno) sredstvo zaštite ljudskih prava i temeljnih sloboda*, FIP – Financije i pravo, Vol. 9, No. 1/2021, pp. 21–52.
12. Uzelac, A., *Pravo na pravično suđenje u građanskim predmetima: Nova praksa Europskoga suda za ljudska prava i njen utjecaj na hrvatsko pravo i praksu*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 60, No. 1/2010, pp. 101–148.

COURT PRACTICE

European Court of Human Rights

1. Černius and Rinkevičius v. Lithuania, nos. 73579/17 and 14620/18, judgment of 18 June 2020.
2. Mamatkulov and Askarov v. Turkey, nos. 46827/99 and 46951/99, judgment of 4 February 2005.
3. Sejdić and Finci v. Bosnia and Herzegovina, nos. 27996/06 and 34836/06, judgment of 22 December 2009.
4. Tolstoy Miloslavsky v. the United Kingdom, no. 18139/91, judgment of 13 July 1995.

5. Dragan Kovačević v. Croatia, no. 49281/15, judgment of 12 May 2022.
6. Marković and Others v. Italy, no. 1398/03, judgment of 14 December 2006.
7. Airey v. Ireland, no. 6289/73, judgment of 9 October 1979.
8. Pham Hoang v. France, judgment of 25 September 1992.
9. Loizidou v. Turkey, no. 15318/89, judgment of 28 November 1996.
10. Bibić v. Croatia, judgment of 13 April 2000.
11. Tomašić v. Croatia, no. 21753/03, judgment of 19 October 2006.
12. Muršić v. Croatia, no. 7334/13, judgment of 20 October 2016.
13. Moskalj v. Croatia, no. 60272/21, judgment of 15 October 2024.

Constitutional Court of the Republic of Croatia

1. Decision no. U-III-1380/2014 of 20 May 2015.
2. Decision no. U-III-3686/2019 of 20 December 2022.
3. Decision no. U-III-1243/2020 of 20 December 2022.
4. Decision no. U-III-2883/2018 of 2 March 2023.
5. Decision no. U-III-5169/2019 of 11 March 2025.

LEGAL RULES

1. Act on the Ratification of the Convention for the Protection of Human Rights and Fundamental Freedoms and Protocols Nos. 1, 4, 6, 7 and 11 thereto (Official Gazette No. 18/1997).
2. Constitution of the Republic of Croatia, Official Gazette Nos. 56/1990, 135/1997, 113/2000, 28/2001, 76/2010, 5/2014.
3. Constitutional Act on the Constitutional Court of the Republic of Croatia, Official Gazette Nos. 99/99, 29/02, 49/02.
4. Enforcement of Prison Sentence Act (Official Gazette Nos. 14/21, 155/23).
5. European Convention for the Protection of Human Rights and Fundamental Freedoms, Official Gazette – International Treaties 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10, 13/17.
6. Statute of the Council of Europe, ETS No. 001.
7. Tariff on Attorneys' Fees and Reimbursement of Costs (Official Gazette Nos. 138/2023, 107/2025).

NETWORK RESOURCES

1. European Court of Human Rights, Country Profile: Croatia, https://www.echr.coe.int/d/cp_croatia_eng, 10 January 2026.

2. European Court of Human Rights, Practice Direction – Just Satisfaction Claims,
https://www.echr.coe.int/documents/d/echr/PD_satisfaction_claims_ENG, 13 January 2026.
3. Rules of Court of the European Court of Human Rights,
<https://uredzastupnika.gov.hr/UserDocsImages/dokumenti/POSLOVNIK/Poslovnik%20ESLJPa.pdf>, 16 January 2026.

UDK: 342.7 : 305-055.34 (594)
316.367.7 (594)
Review paper

Fines Fatimah, PhD student

Géza Marton Doctoral School of Political Science and Law, University of Debrecen,
Hungary

E-mail: finesfatimah@ub.ac.id

ORCID-ID: 0009-0009-8308-7132

SILENCING THE RAINBOW: BETWEEN MORAL PANIC AND THE RIGHT TO DEFEND SOCIAL MORALITY IN INDONESIA

ABSTRACT

Since the early 2000s, there are increasing initiatives to regulate and suppress LGBTQ identities in Indonesia through both national and subnational legislation. These developments have been growing in speed with the spread of global information, which political, religious and moral elites have described as threatening cultural and societal values. This framing has cultivated lasting society fears that views LGBTQ identities as foreign threats warranting state intervention. Aceh's Qanun Jinayat, the only regional legislation applying criminal law to same-sex sexual conduct, is the most obvious step in criminalization. This is only a beginning of the journey, there have been numerous local ordinances, such as Peraturan Daerah (local bylaws), Rancangan Peraturan Daerah (draft bylaws), Surat Edaran Bupati (regent circular letters), and Peraturan Bupati (regent regulations) in several sections of the country with specific measures to limit the expression and the presence of LGBTQ people. Though non-criminal in character, these measures are moral governance practices that institutionalise surveillance, social control, and public stigmatisation.

This paper explains to what extent the influence of social fear of LGBTQ propaganda frames legal morality, and how the implications of Indonesian regulation influence the freedom of LGBTQ individuals' identity. This qualitative legal study considers the debate theory of legal moralism between Devlin's theory and Hart's theory. The article argues that these developments institutionalise a distinctly Devlinian form of law and moral, in which law is justified as a vehicle for enforcing shared public morality and preserving social cohesion, in sharp contrast to Hart's liberal emphasis on autonomy, privacy, and the harm principle as limits to legal coercion. By embedding moral panic within legal structures, the Indonesian state normalises identity suppression despite longstanding traditions of gender diversity.

Keywords: Moral panic, legal morality, LGBTQ rights, local bylaw, identity suppression.

1. INTRODUCTION

Over the past two decades, the regulation of sexuality and gender identity has emerged as one of the most contested arenas of law and governance in many parts of the world. In Indonesia, a Muslim-majority country often celebrated for its cultural pluralism and democratic transition, this contestation has taken a particularly pronounced legal form. Since the early 2000s, a growing number of national and subnational initiatives have sought to regulate and suppress LGBTQ identities through a dense web of criminal and administrative measures. These developments have unfolded in parallel with intensifying anxieties over globalisation, Western cultural influence, and the perceived erosion of religious and societal values.

Political, religious, and moral elites increasingly frame sexual and gender diversity as a foreign threat to Indonesian culture and morality. This framing has produced a sustained moral panic in which LGBTQ identities are no longer treated merely as private differences but are constructed as public dangers warranting state intervention. The enactment of Aceh's *Qanun Jinayat*, the only regional legislation in Indonesia that explicitly applies criminal law to same-sex sexual conduct, represents the most visible manifestation of this moral panic. Yet criminalisation in Aceh is only one part of a broader regulatory trajectory. Across different regions, a wide array of local bylaws (*Peraturan Daerah*), draft bylaws (*Rancangan Peraturan Daerah*), regent circular letters (*Surat Edaran Bupati*), and regent regulations (*Peraturan Bupati*) has introduced specific measures that restrict the presence, expression, and social participation of LGBTQ people. Although these instruments are often formally non-criminal, they operate in practice as mechanisms of moral governance that institutionalise surveillance, social control, and public stigmatisation.

These legal developments raise fundamental questions about the relationship between law and morality, the limits of state power over intimate life, and the position of minority identities within a majoritarian democratic order. They also revive a classic jurisprudential controversy: the debate between H.L.A. Hart and Lord Devlin on the enforceability of morality through law. Devlin famously defended the supremacy of shared public morality as a legitimate foundation for legal coercion, arguing that the preservation of social cohesion justified the criminalisation of conduct deemed morally deviant. Hart, by contrast, insisted that the harm principle and respect for individual autonomy and privacy must strictly limit legal intervention. While this debate originally emerged in mid-twentieth-

century Britain in response to the decriminalisation of homosexuality¹, its normative tensions remain highly relevant for understanding contemporary legal moralism in non-Western and postcolonial contexts.

Despite the growing body of scholarship on LGBTQ regulation, moral panic, and Islamic governance in Indonesia, relatively little attention has been paid to how these developments can be systematically analysed through the lens of the Hart–Devlin debate. Much of the existing literature examines particular laws, social movements, or political actors, but seldom situates Indonesian legal practices within broader theoretical discussions on the legitimacy of enforcing morality through law. This gap limits our ability to fully grasp the normative foundations of current regulatory trends and their implications for rights, citizenship, and legal authority.

The questions in this article are: first, how the social fear of LGBTQ propaganda frames legal morality, and second, how the implications of Indonesian regulation influence the freedom of LGBTQ individuals' identities.

2. METHODS

This research adopts a qualitative method, historical and statute approach, analyses the regulation concerning LGBTQ in Indonesia. The study employs a case study approach, focusing on Indonesia as the subject. Indonesia was chosen as the research object because it offers a unique combination of a plural and decentralised legal system, the strong influence of religious values in public policy, and increasing regulation of LGBTQ+ identities, reflecting the institutionalisation of moral panic. In addition, the contrast between the history of gender diversity and contemporary restrictions makes Indonesia a relevant case for examining the relationship among law, morality, and freedom of identity within the framework of legal moralism.

3. THEORETICAL FRAMEWORK

3.1. Moral panic

Moral panic is sociological concept describing situations in which a condition, episode, person, or group is defined as a threat to societal values and interests,

¹ Devlin, P.: , *The Enforcement of Morals*, Oxford University Press, London 1972, p. 3.

generating anxiety and hostility disproportionate to the actual level of harm. Typically, a moral panic involves the construction of a "folk devil", media exaggeration or distortion of events, political and expert commentary that frames the issue as a serious social problem, and demands for intensified social control or new forms of regulation.² Stanley Cohen defines Moral panic as a condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests; its nature is presented in a stylized and stereotypical fashion by the mass media.³

Rothe & Muzzatti, in efforts to advance the panic framework inspired by both Cohen and Goode & Ben-Yehuda propose the following panic process:

1. Someone or something becomes defined as a threat to values or interests.
2. The threat is depicted in a recognisable form by the media.
3. A rapid build-up of public concern generated hostility.
4. Response from authorities, politicians, and moral entrepreneurs.
5. Panic results in social change.⁴

The following numbered progression, proposed by Critcher, is aligned with those applied to Cohen's definition of moral panic, as illustrated earlier in this chapter:

1. *Emergence*: A form of behaviour is perceived as threatening, creating anxiety that something is wrong, with a narrowed focus on imminent dangers.
2. *Media Inventory*: Preliminary explanations of the threat are mainly articulated via news media. The exaggeration, distortion, prediction, and symbolisation of a threat are created as actors become sensitised to danger.
3. *Moral Entrepreneurs*: Groups or organisations speculate about the nature of the problem and recommend remedies to solve the issue. They offer directions and explanations for why behaviours are taking place.

² French, P., *Moral Panic of Islamist Extremism: Elite-Engineered fear Harming the Hierarchy of Credibility*, Liverpool John Moores University, 2024, p. 25.

³ Sean P. Hier, *Conceptualizing Moral Panic through a Moral Economy of Harm*, *Critical sociology*, volume 28, issue 3, Koninklijke Brill NV, Leiden, 2002, p. 312.

⁴ French, P., op. cit, note 2, 2024, p. 16.

4. *Experts*: Like moral entrepreneurs, experts carry a particular weight which affects how the media define issues. The media also uses expert views to reinforce narratives that are in line with the news distributor's ideological value.
5. *Coping and Resolution*: The reactions of leading actors contain ideas about the required measures (remedies). Current policing powers are exploited and, if deemed insufficient, the demand for extraordinary power increases.
6. *Fade Away*: The panic ends, as '*the condition then disappears, submerges or deteriorates and becomes more visible.*'
7. *Legacy*: Potential short-lasting effects becoming a footnote in history or producing lasting changes in social policy, the law, or society's view of itself.⁵

3.2. Legal Moralism

3.2.1. Patrick Devlin engages in debate about moral and criminal law concerning the decriminalization of homosexuality

Lord Patrick Devlin⁶ is best known for his theory of legal moralism, which supports using law to uphold shared moral standards. He explained his views clearly in *The Enforcement of Morals* (1965), a response to the 1957 Wolfenden Report.⁷ The report suggested decriminalising consensual homosexual acts

⁵ French, P, op. cit. note 2, p. 17.

⁶ Patrick Devlin was born in Chislehurst, Kent in 1905. His father was a Roman Catholic Irish architect from County Tyrone, while his mother was of Scottish Protestant descent from Aberdeen. Devlin was appointed as Lord Justice of Appeal, and a year later he was made Baron Devlin of West Wick in the County of Wilts. After retiring, he served as a senior official at the University of Cambridge from 1966 to 1991.

⁷ The Wolfenden Report is a report of the Departmental Committee on Homosexual Offences and Prostitution. The government set up a committee, chaired by Sir John Wolfenden, to examine laws relating to:

1. Homosexual behaviour between consenting adults in private
2. Street prostitution (especially "soliciting" in public)

The recommendation of the report was that:

1. Homosexual acts between consenting adults in private should no longer be a criminal offence.
2. The law should distinguish between public morality and what adults do in private.

between adults in private, but Devlin disagreed. He believed society has a legitimate interest in protecting its moral values and that law is essential in maintaining social unity.

At the heart of Devlin's theory is the claim that society is bound together by a shared morality. For Devlin, moral norms are not merely private beliefs but constitute the "cement" that holds a society together. If these moral bonds are seriously undermined, society itself is at risk of disintegration. On this view, the protection of public morality is as important as the protection of political institutions or national security. Law is therefore justified in intervening to suppress conduct that threatens the moral fabric of society, even when such conduct occurs in private and does not produce immediate harm to others.

Devlin rejects the "harm principle"⁸ as an adequate limit on legal intervention. He argues that harm should not be understood narrowly as physical injury or direct economic loss. Instead, conduct that deeply offends shared moral sensibilities can itself be considered harmful to society as a whole. Moral outrage, social intolerance, and collective disgust are treated as indicators that a practice poses a threat to social cohesion. From this perspective, legal enforcement of morality is not irrational or oppressive but a necessary response to protect society's moral integrity.

Devlin argues that the Wolfenden Report incorrectly aims for a single simple principle protecting individuals from harm to distinguish crime from sin. He contends that the main purpose of criminal law is not just safeguarding individuals but also preserving society's existence and its shared moral values. There can't be a strict separation between law and morals; criminal law naturally enforces key moral principles. Historically connected to Christian teachings, current law draws its moral foundation from the community's collective sense of right and wrong, which often coincides with Christian morals where law intervenes. He believes society needs both moral guidance, mostly provided by religion, and legal enforcement. Without the moral order rooted in Christian beliefs and common sense, law alone can't sustain social unity. Any effort to limit law to preventing tangible harm while avoiding moral enforcement is both conceptually flawed and inconsistent with actual legal practice.

This led (a decade later) to the Sexual Offences Act 1967 in England and Wales. This partially decriminalized homosexuality between men over 21 in private. Because of this, Lord Wolfenden was then regarded as a hero for the homosexual community.

⁸ Devlin, P., *op. cit.* note 1, p. 11.

Devlin argues that criminal law is grounded in shared moral principles and that society may legitimately use the law to enforce its common morality, including in matters often regarded as purely private. He criticizes the Wolfenden Report for trying to draw a sharp line between protecting the public and enforcing morals. The Wolfenden Report had recommended decriminalizing private, consensual homosexual acts between adults and emphasized individual freedom in private morality. Devlin responds by asking three key questions:⁹

1. Has society the right to pass judgment all on matters of morals?
Ought there, in other words, to be a public morality, or are morals always a matter for private judgement? (whether society has the right to judge matters of morals)
2. If society has the right to pass judgement, has it also the right to use the weapon of the law to enforce it? (if it does, whether it may use criminal law to enforce those judgments)
3. If so, ought it to use that weapon in all cases or only in some and if only in some, on what principles should it distinguish? (if so, when and on what principles it should do so)¹⁰

On Devlin's view, there must be a public morality: a shared set of ideas about good and evil that holds society together. Society is a "community of ideas" not only in politics but also in morals, and without shared moral standards, social disintegration threatens. He uses institutions like marriage to show how political and moral structures are fused. Monogamous marriage is both a moral ideal and a social foundation. Even non-Christians, he notes, are bound by a Christian-based institution of marriage, not because of their religious beliefs, but because it is part of their society's structure and public morality.

Devlin criticizes the Wolfenden Report's language of "private morality" and "individual freedom of choice" because it appears to deny that society may make collective judgments about immorality as such. Yet, he observes, the Report still assumes that homosexuality and prostitution are immoral: it supports laws against the "corruption" of youth and against "immoral earnings," and it treats prostitution as immoral even while leaving the act itself legal, instead criminalizing brothels, pimps, and related activities. To justify these laws, the Report relies on broad ideas such as "corruption and exploitation of others," especially the vulnerable. Devlin argues that such concepts are so elastic that, in principle, they could justify state

⁹ Devlin, P., op. cit. note 1, p. 7.

¹⁰ Devlin, P., op. cit. note 1, p. 7-8.

intervention in almost any form of sexual immorality, thereby undermining the Report's attempt to carve out a protected private sphere.

At the same time, Devlin recognizes that individuals have claims to autonomy. While any immorality can, in his view, injure society, he rejects the idea of two separate spheres—a public morality and a private morality. Instead, there is a single moral sphere that contains both public and private interests, and these must be balanced. He likens this to the shared use of a highway: both the public and the individual driver have rights, but these rights must be mutually curtailed to allow everyone to use the road safely.

Devlin describes the criminal law as embodying a kind of minimum morality. The law should not aim to encode the full moral ideal that citizens might aspire to, but only to set a basic moral floor beneath which conduct will not be tolerated. There must, therefore, be a gap between the moral law and the law of the state. Good citizens should aim higher than the legal minimum. Confusing what is morally right with what should be legally enforced leads, in his view, to mistakes like the Wolfenden Committee's attempt to find a single principle that can neatly separate crime from sin.

Finally, Devlin offers a different account of the true function of criminal law than that suggested by the Wolfenden Committee. While Wolfenden sees criminal law primarily as a device to protect individuals from harm, Devlin argues that the law's fundamental purpose is to protect society itself: its institutions and the shared moral and political ideas that make social life possible. Therefore, society cannot ignore an individual's morality any more than it can ignore his loyalty; both are essential to its survival. At the same time, the examples of adultery and fornication show that the boundary between law and morals is pragmatic. These are practices that can be socially harmful, yet they are left largely outside criminal law because they are difficult and inappropriate to punish. In summary, Devlin maintains that society cannot exist without a common morality, that this morality is defined by the standards of the reasonable, right-minded person, and that while individuals may dissent from these standards, they cannot reasonably insist on complete freedom to act on their dissent when it threatens the moral foundations on which society rests. Society therefore has at least a *prima facie* right to legislate against immorality as such, with the exact reach of the criminal law determined case by case by balancing individual freedom, social necessity, privacy, enforceability, and the strength of public moral feeling.

3.2.2. HLA Hart

H.L.A. Hart is a central figure in modern legal philosophy, best known for his contribution to legal positivism and his critical analysis of the relationship between law and morality. Hart does not deny that law and morality are connected; rather, he argues that moral judgment alone is not sufficient to justify the use of legal coercion. His position is most clearly articulated in *The Concept of Law* (1961) and *Law, Liberty and Morality* (1963), *The Morality of the Criminal law* (1965), *Essay on Bentham: Jurisprudence and Political Theory* (1982), *Essay in Jurisprudence and Philosophy* (1983), where he develops a framework that distinguishes legal validity from moral approval while defending individual liberty against moralistic regulation.

At the core of Hart's theory is the distinction between law and morality. Hart maintains that the existence and validity of a legal rule depend on social facts such as its acceptance by legal officials rather than on its moral content. This distinction allows law to be critically evaluated rather than treated as inherently just. Hart emphasises that recognising immoral laws as legally valid does not endorse them; instead, it enables moral criticism and legal reform.

Hart's critique of legal moralism emerges most clearly in his response to Lord Devlin's argument that society may use law to enforce shared moral standards. Hart rejects the view that moral disapproval or social disgust provides a legitimate basis for criminalisation. Drawing on John Stuart Mill's harm principle, he argues that legal intervention is justified only to prevent harm to others. Private, consensual conduct between adults, particularly in matters of sexuality, falls outside the proper scope of criminal law, even if it offends prevailing moral views. Central to Hart's moral reasoning is the value of individual autonomy. He argues that individuals have a moral right to shape their own lives and make personal choices free from state interference, especially in intimate matters. Hart also stresses the importance of privacy, warning that legal intrusion into private life on moral grounds undermines human dignity and weakens respect for the law. Criminal law, as a coercive and stigmatizing instrument, should therefore be used sparingly and only when clearly justified.

Hart further distinguishes between positive morality and critical morality. Positive morality consists of the moral beliefs actually held by a society, while critical morality involves norms that can be rationally justified. Hart insists that law should not simply enforce majority morality, as social consensus may reflect prejudice rather than moral truth. Using law to impose dominant moral views risks

marginalising minorities and producing what Hart describes as a tyranny of the majority.

Hart challenges claims that society will disintegrate if morality is not legally enforced. He argues that pluralistic societies can tolerate moral diversity without collapsing, and that fear of moral decline often masks discomfort with difference rather than genuine social harm. Overall, Hart's theory offers a liberal and restrained account of legal authority, grounded in respect for autonomy, privacy, and moral diversity. His work remains highly relevant for evaluating laws that regulate identity and sexuality on the basis of moral panic rather than demonstrable harm.

Hart rejected Devlin's claim that violations of conventional morality are sufficiently harmful to justify the regulation of personal conduct by the state. According to Hart, social morality is not a smooth network where its damage can be equated with betrayal. Instead, this morality is considered as parts that need to be questioned whether their enforcement is appropriate for each part. In his three lectures at Stanford, Hart argued differently from Devlin, that a democratic state does not have the right to enforce moral standards for its own interests. Except in certain cases where paternalistic laws are deemed necessary, the state should respect individual freedom and only intervene to prevent or punish actions that truly cause harm. Hart's lecture material at Stanford was later published as the books "Law, Liberty and Morality" (1963) and "The Morality of Criminal Law" (1965).¹¹

4. FINDINGS

4.1. Historical and cultural view of LGBTQ people in Indonesia

Indonesia is one of the world's most populous countries, with its population officially recorded at approximately 286.693.693 people as of mid-2025¹², according to statistics published by Badan Pusat Statistik (BPS), making it the fourth most populous country globally. This large and diverse population spans thousands of islands and includes hundreds of ethnic groups, contributing to a rich

¹¹ Bello, P., *Perluakah Kriminalisasi Terhadap Perilaku Amoral? Perdebatan Patrick Devlin dan H.L. A. Hart*, Jurnal Hukum To-Ra: Hukum untuk Mengatur dan Melindungi Masyarakat, Volume 10, Issue 2/2024, p. 367.

¹² CNN Indonesia, *Jumlah Penduduk Indonesia Naik di 2025, jadi 286 Juta Orang*, <https://www.cnnindonesia.com/edukasi/20250717095433-561-1251652/jumlah-penduduk-indonesia-naik-di-2025-jadi-286-juta-orang>, 29 December 2025.

cultural tapestry and complex demographic structure. The pie chart below illustrates the proportion of the ten largest ethnic groups in Indonesia.¹³

The Javanese ethnic group is by far the largest in Indonesia, accounting for about 40.22% of the total population. They are followed by the Sundanese at 15.50%, making these two groups dominant in Indonesia’s demographic structure. Other major ethnic groups include the Batak (3.58%), Madurese (3.03%), Betawi (2.88%), Minangkabau (2.73%), Buginese (2.69%), and Malay (2.27%), while ethnic groups from Sulawesi and South Sumatra together also contribute significant portions of the population.

The argument that LGBTQ is Western propaganda spreading to Indonesia contrasts with Indonesian culture as evidence, which recognises LGBT identity as an accepted part of society.

NO	ETHNIC	DESCRIPTION
1	Bugis – Makassar	Bugis culture traditionally recognizes five genders: 1. <i>Oroane</i> (men) 2. <i>Makkunrai</i> (women) 3. <i>Calalai</i> (masculine women) 4. <i>Calabai</i> (feminine men) 5. <i>Bissu</i> (androgynous spiritual figures) Bissu is the fifth gender, which embodies all genders or none of them, it transcends gender, it could derive from the Sanskrit word <i>bhiksu</i> , meaning monk. ¹⁴
2	Javanesse- Ponorogo- East Java	“The warok (man of prowess) and his <i>gemblak</i> or <i>janthil</i> (kept boy, who dressed as a woman) are also a phenomenon in Ponorogo in East Java”
3	Javanesse- Yogyakarta	Cross-dressing has long been a common feature of Javanese performing arts. In order to avoid violating prohibitions on physical contact between unmarried male and female dancers, women’s roles in

¹³ Aulia Ulva, Tempo English, *Top 10 Most Populous Countries in the World; Indonesia Ranked 4th*, <https://en.tempo.co/read/1865157/top-10-most-populous-countries-in-the-world-indonesia-ranked-4th>, 29 December 2025.

¹⁴ Pausacker, H., *Homosexuality and the law in Indonesia, Crime and Punishment in Indonesia*, Routledge Law in Asia, New York 2021, p. 474.

		several Javanese dances—at least up until 1914—were often played by men. This was the case in Yogyakarta for dances such as the Bedaya and Wayang Wong, the dance version of wayang kulit, the shadow puppet performance.”
4	Javanese- Surakarta	In Javanese performing arts, cross-dressing has historically been common. To adhere to rules forbidding physical contact between unmarried men and women, female roles in several Javanese dances—up to at least 1914—were performed by men in Yogyakarta. This included dances such as the bedaya and wayang wong, the dance adaptation of the wayang kulit shadow-puppet 400heatre. In contrast, during the late nineteenth century at the Mangkunegaran Court in nearby Surakarta, women took on both male and female roles on stage.
5	Javanese- Surabaya	In ludruk 400heatre, which originates from Surabaya (East Java), female characters are played by male actors. Commenting on this, Peacock notes that ludruk transvestites have traditionally shown more than just a professional interest in portraying feminine roles. Nearly all of them are noticeably effeminate offstage. They wear women’s clothing at home and sometimes even in public, and some go so far as to become the ‘wives’ of men.
6	Bali	In late nineteenth-century Hindu Bali, there was generally a tolerant attitude toward male-male relationships between adult men and youths (referred to as menyelit), as well as toward same-sex relations between women. Historical accounts note that boys around 10–12 years old sometimes cross-dressed as female dancers and, following their performances, had sexual encounters

		with whichever man had placed the highest bid.
--	--	--

Saskia Wieringa¹⁵ observed that same-sex relationships and gender diversity were widely accepted in various regions of Indonesia prior to the colonial period. He further noted that contemporary LGBTQ discrimination constitutes "postcolonial amnesia,' a phenomenon wherein people, in this context the Indonesian populace, forget precolonial customs concerning gender and sexuality following the arrival of Dutch and Portuguese colonizers, who introduced homophobia. Additionally, Wieringa stated that the initial crackdown on homosexuals was executed by Dutch colonial authorities.¹⁶

Wieringa stated that homophobia was introduced by the Portuguese during their occupation of Indonesia in the 16th century. The prevailing conditions in Portugal at that time involved the arrest and burning of individuals engaged in same-sex relations. In the Netherlands, homosexuals could face imprisonment or even the death penalty. When the Dutch arrived, they brought bourgeois morality to various islands and communities in Indonesia, where trans priests were highly respected by their communities. This led the Dutch to believe that there was a necessity for Christianization.

The Dutch colonial government even established a special Morality Police unit (*zedenpolitie*) to arrest homosexual men. This incident became known as the Morality Scandal (*zedenschandaal*). Historian Marieke Bloembergen, in her book *Police During the Dutch East Indies*, writes that between December 1938 and May 1939, police throughout the Dutch East Indies conducted a massive operation against more than 200 men. Most of them were European citizens, including high-ranking officials. They were suspected of having sex with underage boys. This act, both in the Dutch East Indies and the Netherlands, was a criminal offense, even though such a ban had been in effect since 1918. Of the 223 arrested, 171 were found guilty and sentenced. Newspapers followed the raids on homosexuals with rapt attention, as such a large-scale operation had never been conducted before. The campaign was referred to in the news as a "massive housecleaning operation," "moral cleansing," or "cleansing process." Formally, police raids targeted men who had sex with underage boys (under 21). This was regulated under Article 292 of the Dutch East Indies Criminal Code. Paedophilia was a criminal offense.

¹⁵ Professor emeritus of cross-cultural same-sex relationships at Universiteit van Amsterdam, Netherlands.

¹⁶ Berita Tempo, Saskia Wieringa: *Diskriminasi LGBTQ Warisan Kolonialisme*, 22 December 2025, <https://www.tempo.co/teroka/saskia-wieringa-sejarah-gerakan-LGBTQ-kolonialisme-2101262>, 12 January 2026.

However, according to Marieke, these raids actually gave the police the authority to eradicate homosexuality. This was because, before 1938, people were rarely prosecuted for it. "It was also very clear that the police generally targeted homosexuals, especially men," Marieke wrote. After the formation of the Moral Police, homosexuals became the primary target. "Homosexuality was viewed not only as a disgrace that tarnished society's noble morals, but also as a crime".¹⁷

4.2. Today’s law’s perspective on LGBTQ in Indonesia

The following are some rules that emerged after the 1998 reform in Indonesia. The trend of restrictions based on identity has become common in various regional regulations, and some examples of these regulations can be seen in the following column,

NO	REGION	TYPE OF REGULATION	REGULATION NUMBER/YEAR	DESCRIPTION OF CONTENT	CLASSIFICATION
1	Pariaman City	PERDA/ local Regulation	10/2018	Prohibition of LGBTQ behavior (Articles 24–25)	Explicit
2	Cianjur Regency	PERDA/local regulation	1/2020	Use of implicit terminology associated with LGBTQ	Implicit
3	Bogor City	PERDA/ local regulation	10/2021	Implicit provisions encompassing LGBTQ-related conduct	Implicit
4	Aceh	QANUN	6/2014	Criminalization of same-sex relations	Explicit
5	Cianjur Regency	PERDA/ local regulation	1/2020	-	Explicit
6	Tasikmalaya	PERDA/local Regulation	12/2009	Regulation of social life based on Islamic values and norms	Explicit, Regional Regulation of Tasikmalaya Number 12 of 2009 on Development of Life values in Societies according to Islamic Values and Social Norms in Tasikmalaya ¹⁸

¹⁷ Risa Herdahita Putri, *Razia Homoseksual Zaman Kolonial*, <https://www.historia.id/article/razia-homoseksual-zaman-kolonial>, 7 January 2026.

¹⁸ In article 5 "every Muslim is obliged to prevent and avoid despicable acts and actions that can cause loss and collapse of morals, morals and social morals." Disgraceful acts as referred to in paragraph (3), include, among others, the following: a. criminal acts of

7	Province of south sumatera	PERDA/local Regulation	13/2002	-	Regional Regulation of the Province of South Sumatera Number 13 of 2002 on Indecency Eradication in the Province of South Sumatera;
8	Palembang City	PERDA/local Regulation	2/2004	-	Regional Regulation of Padang Panjang Number 9 of 2010 on Amendment of Regional Regulation of Padang Panjang Number 3 of 2004 on Prevention, Eradication, and Prosecution for Indecent Behaviours in Society
9	Padang Panjang	PERDA/local Regulation	9/2010	-	Explicit
7	Makasar City	RAPERDA/ draft local regulation	-	-	-
8	Garut Regency	RAPERDA/ draft local regulation	-	-	-
9	Bandung Regency	RAPERDA/ draft local regulation	-	-	
10	Medan City	RAPERDA/ draft local regulation	-	-	
11	Hulu Sungai Selatan	RAPERDA/ draft local regulation	-	-	
13	Bekasi Regency	Regent Regulation (<i>Peraturan Bupati</i>)	102/2020	LGBTQ defined as a form of sexual deviation	-
14	Cianjur Regency	Surat Edaran/ Circular Letter	2018	-	-
15	Garut Regency	Aturan Ketertiban / Public Order Regulation	-	-	

corruption and abuse of position/power; b. adultery and prostitution, whether committed by people of the opposite sex or by people of the same sex (homosexuals/lesbians)

5. DISCUSSION

5.1. From moral panic to legal moralism: explaining the Indonesian regulatory trajectory

Coined in 1972, the term Moral Panic was first meant to describe how the public comes to a collective panic over threats to societal traditions and values. Moral Panics can be initiated by Interest Groups, Elites, or Grassroots groups.¹⁹ Moral panic is a sudden, strong feeling of fear in a society or other group that something or someone bad will destroy morals (standards for character and behaviour).²⁰

In Indonesia, moral panic is expressed in various ways, starting from request for judicial review submitted to the Constitutional Court with the arguments of protecting children and grandchildren/descendants from the moral decline that is occurring in Indonesia. In **2016, the Constitutional Court of Indonesia (Mahkamah Konstitusi)** became a focal point of broader efforts to criminalise same-sex relations through judicial interpretation of the Criminal Code (KUHP).²¹ A coalition of conservative groups, notably *Aliansi Cinta Keluarga* (Family Love Alliance), filed a **constitutional review (judicial review)** requesting that the Court interpret and expand certain KUHP provisions so that consensual sexual relations between adults of the same sex could be criminalised. In particular, the petition sought to reinterpret Article 292 of the KUHP—originally focused on lewd acts involving minors—and extend its application to **consensual homosexual acts between adults**, effectively creating criminal liability for homosexuality.²² Although the Court ultimately rejected the petition, the arguments advanced by the applicants reveal a distinctly Devlinian logic. Homosexuality was framed as a moral danger capable of corrupting youth, undermining family values, and threatening the moral foundations of Indonesian society. These claims did not rely on demonstrable harm to specific individuals, but rather on the perceived erosion of collective morality. The reason of the judicial review applicant are rejected on the Hart perspective, Hart explicitly rejected the

¹⁹ Thomson, Shery, Moral Panic, <https://www.ebsco.com/research-starters/social-sciences-and-humanities/moral-panic>, 15 January 2026.

²⁰ Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/moral-panic>, 15 January 2026.

²¹ Fines Fatimah, *Discourse on Legality of LGBT from the Perspective of Islamic Law and Indonesian Law*, Academic Journal of Business, Administration, Law and Social Sciences, IIPCCCL Publishing, Graz- Austria, Vol 5/2, July, 2019, p. 2.

²² Human Right Watch, Indonesia: Court Reviews Anti- LGBTQ Law, *Criminalizing Same-Sex Relations Raises Privacy, Discrimination Concerns*, <https://www.hrw.org/news/2016/08/23/indonesia-court-reviews-anti-lgbtq-law>, 15 January 2026.

idea that moral disapproval or social disgust constitutes harm. He warned that allowing law to enforce majority morality risks transforming legal authority into an instrument of moral tyranny. From a Hartian perspective, the attempt to criminalise consensual same-sex relations through judicial interpretation represents an unjustified intrusion into private life, unsupported by evidence of harm and incompatible with principles of autonomy and privacy.

Not only that, the making of regional Regulations is also experiencing a trend, namely the explicit use of the Islamic religion in Regional Regulations, the drafting of regional regulations is also ongoing to date and not only targets same sex sexuality/sexual activity but also limits the expression of their identity, namely restrictions or WARIA (the term for biological men who dress and behave like women).²³ in some areas in Indonesia WARIA are prohibited from appearing in public spaces on TV and so on. The Gorontalo Regency Government held a Regional Leadership Coordination Forum of Gorontalo Regency. The results of this forum were then approved in Circular Letter Number 800/BKBP/76/IV/2025 Concerning the Prohibition of Crowded Public Entertainment Activities and Party Celebrations Involving Transvestites, Singers, Alcohol, Drugs and Gambling which was signed by the Acting Regional Secretary on behalf of the Regent of Gorontalo on April 25, 2025.²⁴

Aceh's *Qanun Jinayat* stands as the most explicit institutionalisation of Devlinian legal moralism in Indonesia. By criminalising same-sex sexual conduct and prescribing corporal punishment, the Qanun translates moral condemnation directly into criminal sanction. This move exemplifies Devlin's argument that criminal law serves not merely to prevent harm but to preserve the moral fabric of society. In Aceh, the moral authority of religious norms is treated as sufficient justification for legal coercion, even in cases involving consensual conduct between adults.

At the National level, the identity of WARIA is recommended to be strictly prohibited through the MUI Fatwa,²⁵ whose recommendations are given sufficient

²³ Circular Letter Number 800/BKBP/76/IV/2025 Concerning the Prohibition of Crowded Public Entertainment Activities and Party Celebrations Involving Transvestites, Singers, Alcohol, Drugs and Gambling in Gorontalo.

²⁴ See <https://lbhmasyarakat.org/pelarangan-menjadi-waria-di-gorontalo-surat-edaran-yang-membuka-keran-diskriminasi/>, 15 January 2026.

²⁵ Fatwa MUI is a religious opinion or ruling issued by the Indonesian Ulama Council (MUI) regarding Islamic law on contemporary issues like food (halal), finance, cosmetics, and social issues. While non-binding by law, they hold significant moral and social authority among Indonesian Muslims and often influence government policy. See <https://fatwamui.com/storage/278/21.-Kedudukan-Waria.pdf>, 15 January 2026.

attention by policymakers in Indonesia. The MUI (Indonesia council of Ulama) Fatwa Commission in its session on 9 Jumadil Akhir 1418 H, coinciding with 11 October 1997 on the issue of transgenders, issued a fatwa:

- a. Transgenders are men and cannot be considered as a separate group (gender).
- b. All deviant behavior of transgenders is haram and must be attempted to return to their original nature. I am running a few minutes late; my previous meeting is running over.

This Fatwa MUI Appeal to two things, there is:

- a. The Indonesian Ministry of Health and the Indonesian Ministry of Social Affairs to guide transgenders to become normal people, by involving psychologists.
- b. The Indonesian Ministry of State Affairs and other related agencies to disband transgender organizations.²⁶

According to Ainun Najib²⁷, the MUI's position within the Indonesian state administration is actually within the state infrastructure. The MUI is an organization of Islamic scholars tasked with empowering the Muslim community. This means that the MUI exists within the community, not a state-owned institution or a representative of the state.

The MUI's fatwas are not state laws with sovereignty imposed on all citizens. They also carry no sanctions and do not require obedience from all citizens. As a socio-political force within the state infrastructure, MUI fatwas are binding and are only obeyed by the Muslim community that feels a connection to the MUI itself. The legality of MUI fatwas cannot compel obedience by all Muslims. Fatwas themselves are essentially nothing more than opinions and thoughts from individual scholars or religious institutions, which may be followed or ignored altogether.²⁸ However, even though the MUI fatwa is not a type of legislation recognized in Indonesia, the existence of this fatwa is often legitimized through regulations by government institutions so that it must be obeyed by the community.²⁹

²⁶ See <https://fatwamui.com/storage/278/21.-Kedudukan-Waria.pdf>, 15 January, 2026.

²⁷ Ainun Najib is an Indonesian Islamic scholar.

²⁸ Fatwa Majelis Ulama Indonesia dalam Perspektif Pembangunan Hukum Responsif, dalam *Kedudukan Fatwa MUI dalam Sistem Hukum Indonesia*, <https://www.hukumonline.com/klinik/a/kedudukan-fatwa-mui-dalam-hukum-indonesia-lt5837dfc66ac2d/>, 15 January, 2026.

²⁹ Yeni Salma, *Kedudukan Fatwa DSN dalam Sistem Hukum nasional*, <https://www.hukumonline.com/klinik/a/kedudukan-fatwa-mui-dalam-hukum-indonesia-lt5837dfc66ac2d/>, 15 January, 2026.

In conclusion, widespread fears—of moral decline, changing social values, and the influence of foreign cultural norms—have prompted even the smallest social groups to urge the state to intervene and regulate morality. Yet many of these matters should not fall under state control, much less be subject to criminal punishment. Morality is largely a family concern. The fear that homosexual ideas will corrupt children is excessive, especially when used to justify state interference. Instead, parents and families should bear primary responsibility for addressing such worries and calming moral panic. When they do not, society becomes overly reactive and pushes for the criminalization of homosexual or LGBTQ individuals in Indonesia. At present, Indonesia tends to prioritize morality defined by the majority, which worsens conditions for minorities judged by those dominant moral standards.

5.2. Implication for identity freedom

The trend, or flurry of regulations at both regional and national levels, criminalizes LGBTQ individuals, both for their sexual activity and for widespread discrimination against this group, making them afraid to reveal their identity. In the workplace, this is still taboo, and they are often avoided. A very explicit example is in the military, where strict rules prohibit same-sex acts by military officers³⁰, which can lead to dismissal from military service and imprisonment.³¹

The growing expression of LGBTQ groups, with the emergence of more and more movements, and research into organizations supporting LGBTQ are currently considered Western propaganda aimed at eradicating the nation's cultural and moral values³². However, it is worthwhile to look back and see that diverse identities, not solely consisting of men and women, have been recognized and become part of the Bugis culture. This may have been introduced through Bugis culture, but it cannot be generalized to reflect on Indonesian cultural values. Bugis culture does not represent that.

³⁰ Surat Telegram Panglima TNI (Telegram from the Commander of the Indonesian National Armed Forces) Nomor ST/398/2009 tanggal 22 Juli 2009 and Surat Telegram Panglima TNI Nomor ST/1648/2019 tanggal 22 Oktober 2019

³¹ Under Article 103 juncto Article 26 KUHPM (Indonesian Military Criminal Code) as an administrative legal measure.

³² Nursyahbani & Saskia Wieringa, *Creeping Criminalisation (Mapping of Indonesia's Laws and Regional Regulations that Violate Human Rights of Women and LGBTIQ People)*, Outright Action International, New York, 2016, p. 88.

The cumulative effect of judicial reviews, criminal regulations, administrative bylaws, and moral directives is a legal environment in which LGBTQ identity is systematically constrained. Individuals face exclusion from employment, education, public space, and political participation, not because of harmful conduct, but because their identities are framed as morally unacceptable. This configuration normalises identity suppression and transforms moral panic into durable governance.

From a Devlinian perspective, these outcomes may be defended as necessary sacrifices to preserve social cohesion. Yet Hart's theory exposes the cost of such sacrifices: the erosion of individual autonomy, the marginalisation of minorities, and the transformation of law into an instrument of moral conformity. The Indonesian case thus illustrates the enduring relevance of the Hart–Devlin debate beyond its original British context. It shows how Devlinian legal moralism, when combined with moral panic, can flourish within contemporary plural legal systems, particularly where religious and cultural authority are deeply embedded in governance.

6. CONCLUSION

The regulation of LGBTQ identities in Indonesia results from a sustained moral panic that has become increasingly institutionalised through legal and administrative means at both national and local levels. Judicial review petitions before the Constitutional Court, Aceh's *Qanun Jinayat*, the proliferation of *Peraturan Daerah* and *Rancangan Peraturan Daerah*, executive circular letters, regent regulations, and the normative influence of religious fatwas collectively create a legal environment where LGBTQ identities are seen as moral threats rather than rights-bearing individuals. Although only Aceh formally criminalises same-sex conduct, administrative and semi-legal instruments elsewhere serve as effective tools of moral governance, limiting expression, visibility, and participation in public life. These measures do not aim to prevent actual harm but to uphold dominant moral values, resulting in systemic discrimination, self-censorship, and exclusion from employment, education, and state institutions such as the military.

Analysed through the Devlin–Hart framework, Indonesia's regulatory trajectory reflects a predominantly Devlinian logic in which the preservation of perceived social cohesion justifies extensive legal intervention into private life. Moral disapproval, rather than harm, is treated as a sufficient basis for regulation, allowing law to become an instrument for enforcing conformity. Hart's liberal

critique, however, reveals the costs of this approach: the erosion of individual autonomy, the marginalisation of minorities, and the weakening of legal restraint in plural societies. The Indonesian case thus illustrates how legal moralism, when combined with moral panic and reinforced by religious and cultural authority, can flourish within a decentralised legal system while normalising identity suppression. It underscores the urgent need to reaffirm harm-based reasoning, constitutional protections, and respect for diversity as limits on the moral reach of law.

REFERENCE

BOOKS AND ARTICLES

1. Bello P, Perlukah Kriminalisasi Terhadap Perilaku Amoral? Perdebatan Patrick Devlin dan H.L.A. Hart, *Junral Hukum To-Ra: Hukum untuk Mengatur dan Melindungi Masyarakat*, Volume 10 Issue 2, 2024.
2. Devlin P, *The Enforcement of Morals*, Oxford University Press, 1972.
3. Fatimah F, *Discourse on Legality of LGBT from the Perspective of Islamic Law and Indonesian Law*, *Academic Journal of Business, Administration, Law and Social Sciences*, IIPCCCL Publishing, Graz- Austria, Vol 5/2, July, 2019.
4. French P, *Moral Panic of Islamist Extremism: Elite-Engineered fear harming the Hierarchy of Credibility*, Liverpool John Moores, 2024.
5. Hart HLA, *The Concept of Law*, New York: Clarendon Press- Oxford, 1997.
6. Nursyahbani, *Creeping Criminalisation (Mapping of Indonesia's Laws and Regional Regulations that Violate Human Rights of Women and LGBTIQ People)*, Outright Action International, New York, 2016.
7. Pausacker H, *Homosexuality and the law in Indonesia, Crime and Punishment in Indonesia*, Routledge Law in Asia, 2021.
8. Wieringa S, *Sexual Politics in Indonesia*, Palgrave Macmillan, New York, 2002.
9. Wieringa S, *A Political Biography of the Indonesian Lesbian, Bisexual and Trans Movement*, Bloomsbury Academic, Great Britain 2024.
10. Wieringa S, *Criminalisation of Homosexuality in Indonesia: The Role of the Constitution and Civil Society*, *Australian Journal of Asian Law*, 2019, Vol 20 No. 1.

LEGAL ACTS

1. Circular Letter Number 800/BKBP/76/IV/2025 Concerning the Prohibition of Crowded Public Entertainment Activities and Party Celebrations Involving Transvestites, Singers, Alcohol, Drugs and Gambling in Gorontalo.
2. Surat Telegram Panglima TNI (Telegram from the Commander of the Indonesian National Armed Forces) Nomor ST/398/2009 tanggal 22 Juli 2009
3. Surat Telegram Panglima TNI Nomor ST/1648/2019 tanggal 22 Oktober 2019.

NETWORK RESOURCES

1. Berita Tempo, Saskia Wieringa: Diskriminasi LGBTQ Warisan Kolonialisme, 22 December 2025, <https://www.tempo.co/teroka/saskia-wieringa-sejarah-gerakan-LGBTQ-kolonialisme-2101262>, 12 January 2026.
2. Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/moral-panic>, 15 January 2026.
3. CNN Indonesia, <https://www.cnnindonesia.com/edukasi/20250717095433-561-1251652/jumlah-penduduk-indonesia-naik-di-2025-jadi-286-juta-orang>, 29 December 2025.
4. Fatwa Majelis Ulama Indonesia dalam Perspektif Pembangunan Hukum Responsif, dalam Kedudukan Fatwa MUI dalam Sistem Hukum Indonesia, <https://www.hukumonline.com/klinik/a/kedudukan-fatwa-mui-dalam-hukum-indonesia-lt5837dfc66ac2d/>, 15 January, 2026.
5. Human Right Watch, Indonesia: Court Reviews Anti- LGBTQ Law, Criminalizing Same-Sex Relations Raises Privacy, Discrimination Concerns, <https://www.hrw.org/news/2016/08/23/indonesia-court-reviews-anti-LGBTQ-law>, 15 January 2026.
6. Kedudukan Fatwa DSN dalam Sistem Hukum nasional, disertasi Yeni Salma, , <https://www.hukumonline.com/klinik/a/kedudukan-fatwa-mui-dalam-hukum-indonesia-lt5837dfc66ac2d/>, 15 January, 2026.
7. Kedudukan Waria, <https://fatwamui.com/storage/278/21.-Kedudukan-Waria.pdf>, 15 January 2026.
8. Moral Panic, <https://www.ebsco.com/research-starters/social-sciences-and-humanities/moral-panic>, 15 January 2026.
9. Pelarangan menjadi Waria di Gorontalo: Surat Edaran yang membuka Keran Diskriminasi, <https://lbhmasyarakat.org/pelarangan-menjadi-waria-di-gorontalo-surat-edaran-yang-membuka-keran-diskriminasi/>, 15 January 2026.

10. Razia Homoseksual Zaman Kolonial, Risa Herdahita Putri, *Historia*, 9 Marte 2019, <https://www.historia.id/article/razia-homoseksual-zaman-kolonial>, 7 January 2026.
11. The Most Populous Countries in the World; Indonesia, ranked 4, <https://en.tempo.co/read/1865157/top-10-most-populous-countries-in-the-world-indonesia-ranked-4th>, 29 December 2025.

UDK: 347.77 (597)
339.13 (597)
Professional paper

Nguyen Thi Hang Diem Mi, PhD student

Doctoral School of Law and Political Sciences, University of Szeged, Hungary

E-mail: nthdmi@ctu.edu.vn

ORCID-ID: 0009-0002-9579-9574

THE ACTUAL SITUATION OF VIETNAM'S GI LEGAL FRAMEWORK AND THE MEASURES FOR ITS MAINTENANCE AND DEVELOPMENT

ABSTRACT

The Vietnamese legal framework concerning geographical indications (GIs) has been established since the 1990s and is currently being adapted in an attempt to better align with international law. Over the years, GIs in Vietnam have significantly contributed to the national economic growth and the preservation of traditional heritage. However, the GI system in Vietnam has not been fully exploited and does not adequately reflect the country's economic prosperity, particularly in agriculture and handicrafts sectors. The main objective of this research is to discuss the current issues that GIs in Vietnam are now facing, focusing on those stemming from the legal framework. We primarily employ the comparative and analytical method to identify the differences and similarities between the EU and Vietnam's legislations on GIs. To this end, we extract the valuable lessons that Vietnam can learn from the EU to harmonize its law with international standards and strengthen its GI regulations.

Keywords: *Actual situation, geographical indication, legal framework, Vietnam, EU*

1. INTRODUCTION

Geographical indication (GI) under Vietnamese law is defined as an indicator of geographical origin of goods originating in specified region, locality, territory, or country.¹ The first Vietnamese law recognizing GIs was the 1995 Civil Code, which stated that GI is a sign identifying a product that originates from a specific area, locality, region or country². Actually, GI was enacted like scheme by Vietnamese government in 1989 through the Ordinance on the Protection of Industrial Property Rights. However, this scheme remained in hibernation until

¹ Article 4 (22), Vietnam's Intellectual Property Law of 2005.

² Article 768 of the Civil Code 1995.

2001, when the first two GI products – Phu Quoc Fish sauce and Shan Tuyet Tea from Moc Chau – were registered.³ In 2005, Vietnam's Intellectual Property Law (hereinafter the 2005 IP Law) was enacted, demonstrating Vietnamese government's effort to comply with the WTO's Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS). Vietnamese GIs have actually turned over a new leaf when the EU-Vietnam Free Trade Agreement (EVFTA) entered into force in August 2020 with specific commitments on GIs. EVFTA opens the door for 39 Vietnamese GIs⁴ to be protected in the EU, allowing these products to enter a single market. However, to align with the EU's standards, Vietnam is also required to adjust its GI legal framework, leading to the third amendments of the 2005 IP Law in June 2022.

In practice, the protection, management, maintenance and improvement of Vietnam's GI system are now facing a lot of problems, stemming from various reasons. For example, the issue caused by the current administrative restructure that took place in April 2025 has negatively impacted the situation for the Vietnamese GIs. Specifically, according to the Article 1(2) of the Resolution No.76/2025/UBTVQH15, dated April 14, 2025, the rearrangement of province-level administrative divisions means merging provinces with other provinces to establish new provinces, or merging provinces with centrally-affiliated cities to establish new centrally-affiliated cities, as approved by the competent authorities, in order to reduce the number of administrative divisions, increase their scale, and expand development space. As a result of this restructuring, operation of district-level administrative divisions nationwide shall be terminated from July 01, 2025⁵, leading to the removal of numerous provinces and cities from the administrative map. Consequently, many GIs pertained to such eliminated provinces face the risk of confusion regarding the origin of their products, potentially damaging their reputation. Another challenge facing Vietnam's GI system is the limited involvement of GI producers in the development of product specification, the GI application process, and management. Additionally, there is the lack of development for geographical indication related to craft and industrial products despite the country's rich tradition handicraft and craft villages. Furthermore, insufficient attention to sustainability in legislation could negatively impact the competitiveness of Vietnam's GI-protected products in the international market.

³ Nguyen, S L.; Le, V A., *Diffusion of Geographical Indication Law in Vietnam: "Journey To The West"*, IIC, 2023, 176-199, p. 179, available at <https://doi.org/10.1007/s40319-023-01289-9>.

⁴ Chapter 12, EVFTA, available at https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/viet-nam/eu-viet-nam-agreements/texts-agreements_en (accessed on September 4, 2025).

⁵ Article 2 (2), Resolution No.203/2025/QH15 amendments to certain articles of the Constitution of the Socialist Republic of Vietnam.

This chapter aims to draw the lesson for Vietnam based on the EU's approach to GIs, with the goal of strengthening the Vietnam's GI system. To achieve that goals, the comparative and analytical method will be primarily employed.

Overall, the chapter contains the view that although Vietnam's GI system has made significant progress, it still necessitates structural refinement, enhanced participation of producer groups, the incorporation of sustainability principles, and more responsive administrative mechanisms.

2. THE BRIEF OVERVIEW OF THE EU'S REGULATIONS REGARDING GIs

Under EU law, geographical indication refers to a sign identifying a product as originating from a particular territory where its quality, characteristics, or reputation are essentially attributable to its geographical origin.⁶

Regarding the EU's GI system, this consists of three main categories: Protected Designation of Origin (PDOs), Protected Geographical Indication (PGIs), and Geographical Indication (GIs). PDO and PGI are designed to protect foodstuffs and wines, while GI specifically applies to spirits.⁷

The EU's GI system has been reformed and four main key pillars are the strength of the role of producer groups, the effective protection, the simplification of the registration system, and the sustainability and transparency.⁸ Regarding the GI producer groups, their responsibilities extend beyond merely safeguarding the name of the product. These groups are involved in drafting and revising the product specification, submitting application for registration, amendments, or cancellation, and acting on behalf of their members within intellectual property enforcement frameworks, including cooperation with national and EU-level anti-counterfeiting authorities. In addition, producer associations are expected to enhance the overall value and long-term viability of the GI. This includes

⁶ Article 5 of Regulation (EU) No 1151/2012 of the European Parliament and of the Council on quality schemes for agricultural products and foodstuffs.

⁷ Geographical indications and quality scheme explained, available at https://agriculture.ec.europa.eu/farming/geographical-indications-and-quality-schemes/geographical-indications-and-quality-schemes-explained_en#pdo (accessed on September 10, 2025).

⁸ Adinolfi, F.; Vecchio, Y.; Masi, M.; Mastandrea, G.; Lambertini, G.; De Castro, P., (2024). *The reform of EU geographical indications: A look at the newly approved Regulation*, *AIMS AGRICULTURE AND FOOD*, 2024, 693-698, p.695-696, available at <https://doi.org/10.3934/AGRFOOD.2024037>.

strengthening environmental protection, social responsibility, and economic sustainability linked to the product. They also play a proactive role in detecting and addressing infringement or misleading commercial practices, ensuring that products marketed under the GI comply with the approved specification.⁹ When it comes to the sustainable practices, producer groups may draft and periodically update a sustainability report supported by verifiable data. Such a report typically outlines the sustainable practices applied in production, evaluates how production methods affect environmental, social, economic, or animal welfare objectives, and explains how these factors influence the product's development, market performance, and reputation. The European Commission is responsible for publishing this report to ensure transparency.¹⁰

3. BRIEFING THE VIETNAM'S GI LEGAL FRAMEWORK

Vietnam's GI law is built primarily on the Law on Intellectual Property No.50/2005/QH11 of November 29, 2005, of the XI National Assembly (2005 IP Law) and its amendments (2009, 2019, and 2022), detailed through Government's Decree No. 65/2023/ND-CP of August 23, 2023, detailing a number of articles of, and providing measures to implement the law on Intellectual Property regarding industrial property, protection of industrial property rights and plant variety rights, and the state management of intellectual property (Decree 65), Government's Decree No. 105/2006/ND-CP of September 22, 2006, detailing and guiding the implementation of a number of articles of the law on intellectual property on protection of Intellectual property rights and on State management of Intellectual Property (Decree 105), and Ministry of Science and Technology's Circular No. 23/2023/TT-BKHCT of November 30, 2023 (Circular 23), detailing a number of articles of the Law on Intellectual Property and providing measures to implement Decree 65 related to procedure for establishment of intellectual property rights and assurance of industrial property information. Additionally, the GI system of Vietnam is strongly influenced by international commitments, including TRIPS Agreement, and EVFTA.

In general, the majority of the Vietnam's regulations on GIs align with those of the European Union. This includes aspects such as the definition of GIs, homonymous

⁹ Article 32 of the Regulation (EU) 2024/1143 of the European Parliament and of the Council on geographical indications for wine, spirit drinks and agricultural products, as well as traditional specialties guaranteed and optional quality terms for agricultural products, amending Regulations (EU) No 1308/2013, (EU) 2019/787 and (EU) 2019/1753 and repealing Regulation (EU) No 1151/2012.

¹⁰ Article 8 of the Regulation (EU) 2024/1143.

GIs, the conditions for GI protection, and the registration procedures. According to the Article 11 of the Vietnam's 2022 IP Law, a geographical indication is a sign used to indicate the geographical origin of products originating from a specific area, locality, territory, or country. This definition corresponds to the criteria set forth in the Article 22(1) of the General Agreement on Tariff and Trade (GATT;1994), which offers a minimum standard and a comprehensive definition of GI without limiting it to any particular category.¹¹ Additionally, a recent amendment added a new Clause 22a to Clause 22 of Article 4 of the 2005 IP Law, which defines a homonymous geographical indication as a geographical indication that has the same pronunciation or spelling.

The main difference between Vietnam and the EU in regulating GIs is the role of GI producers. Under EU's law, producer groups play a key role in creation, registration, management, and maintenance GI system. For instance, Article 32 of the Regulation (EU) 2024/1143 sets out the functions assigned to recognized producer groups. These include the preparation of the product specification, the submission of applications for registration as well as for amendments or cancellation, and the implementation of activities aimed at managing the geographical indication. Producer groups are also expected to assist their members in establishing internal control mechanisms to monitor and ensure conformity with the approved specification. Furthermore, they are required to take appropriate measures to safeguard the geographical indication and the intellectual property rights associated with it. However, producers of Vietnamese GI-protected products tend to play a relatively limited role in the formation of product specifications, the registration for protection and the GI management. This position causes by the Vietnam's top-down approach to GIs. The state authorities play prominent role in GI application for registration, and in the elaboration of product specification as well as setting rules for GI practices, leaving no space for producers and other stakeholders to express their opinions on their products and the formation of GIs.¹² Under the GI law of Vietnam, GIs belong to the State, and public authorities play a key part in the creation and management of GIs.¹³ The other difference between the two GI law systems is the regulation regarding the sustainability. According to the Article 8 of the Regulation (EU) 2024/1143, farmers shall agree with the

¹¹ Nga, T H.; Nguyen, N K H, *Protection of non-agricultural geographical indications under EU law: implications for the EVFTA and compatibility with Vietnam's intellectual property legislation*, TalTech Journal of European Studies, 2025, 25-39, p30, available at <https://doi.org/10.2478/bjes-2025-0018>.

¹² Pick, B.; Marie-Vivien, D., *Representativeness in Geographical Indications: A Comparison between the State-Driven and Producer-Driven Systems in Vietnam and France*, Sustainability, 2021, 1-16, p.5, available at <https://doi.org/10.3390/su13095056>.

¹³ Article 121(4), 2005 IP Law.

sustainable practices. Therefore, they must comply with the sustainable agreement to produce products bearing GIs, prepare and regularly update a sustainable report that demonstrates their compliance. In contrast, Vietnam’s current IP law lacks specific provisions for sustainability. Furthermore, there are no requirements for farmers to regularly report on their implementation of sustainable practices in producing GI-labelled products, indicating a lack of emphasis on sustainability.

4. THE ACTUAL STATUS OF VIETNAMESE Gis

From 2001 to 2024, there were 137 products have been protected as geographical indication in Vietnam (see Table 1)

Table 1. The official list of GI-designated products in Vietnam from 2001 to 2024

List of Geographical Indications in Vietnam from 2001 to 2024						
No	Filing Number	Registration Number	Registration Date	Geographical Indication	Products	Applicant
1	6-2001-00001	6-00001	01.06.2001	Phủ Quốc	Phu Quoc Fish sauce	Association
2	6-2001-00009	6-00002	09.08.2010	Mộc Châu	Shan Tuyet Tea	Department of Science and Technology of province Son La
3	6-2001-00002	6-00003	13.05.2002	Cognac	Spirit	National interagency office Cognac
4	6-2005-00001	6-00004	14.10.2005	Buôn Ma Thuột	Coffee	Provincial People’s Committee - Đắk Lắk
5	6-2006-00001	6-00005	08.02.2006	Đoan Hùng	Pomelo	Department of Science and Technology of province Phú Thọ
6	6-2004-00003	6-00006	15.11.2006	Bình Thuận	Dragon Fruit	Association
7	6-2006-00003	6-00007	15.02.2007	Lạng Sơn	Star Anise	Department of Science and Technology of province Lạng Sơn
8	6-2006-00002	6-00008	23.05.2007	Pisco	wine	Peru
9	6-2006-00005	6-00009	25.05.2007	Thanh Hà	Lychee	People’s Committee – District Thanh Hà
10	6-2004-00001	6-00010	30.05.2007	Phan Thiết	Fish sauce	Department of Standards, Metrology and Quality of Bình Thuận province
11	6-2006-00004	6-00011	31.05.2007	Hải Hậu	Rice	Association
12	6-2007-00001	6-00012	31.05.2007	Vinh	Organ	Department of Science and Technology of province Nghệ An
13	6-2007-00004	6-00013	20.09.2007	Tân Cương	Tea	Department of Science and Technology of province Thái Nguyên

14	6-2007-00002	6-00014	25.06.2008	Hồng Dân	Rice	Department of Science and Technology of province Bạc Liêu
15	6-2008-00001	6-00015	25.06.2008	Lục Ngạn	Lychee	Department of Science and Technology of province Bắc Giang
16	6-2003-00009	6-00016	03.09.2009	Hòa Lộc	Mango	Department of Science and Technology of province Tiền Giang
17	6-2008-00004	6-00017	30.09.2009	Đại Hoàng	Banana	People's Committee – Distric Lý Nhân
18	6-2009-00001	6-00018	07.01.2010	Văn Yên	Cinnamon Bark	People's Committee – Distric Văn Yên
19	6-2008-00007	6-00019	25.06.2010	Hậu Lộc	Fermented Shrimp Paste	People's Committee – Distric Hậu Lộc
20	6-2009-00005	6-00020	19.07.2010	Huế	Conical Hue	Department of Science and Technology of province Thừa Thiên Huế
21	6-2010-00003	6-00021	08.09.2010	Bắc Kạn	Seedless Persimmon	Department of Science and Technology of province Bắc Kạn
22	6-2009-00002	6-00022	09.11.2010	Phúc Trạch	Pomelo	People's Committee – Distric Hương Khê
23	6-2008-00003	6-00023	19.11.2010	Scotch whisky	Spirit	The Scotch Whisky Association
24	6-2009-00004	6-00024	19.11.2010	Tiên Lãng	Lao Tobacco	People's Committee – Distric Tiên Lãng
25	6-2008-00008	6-00025	10.01.2011	Bảy Núi	Fragrant rice Nang Nhen	People's Committee – Distric Tĩnh Biên
26	6-2010-00002	6-00026	21.03.2011	Trùng Khánh	Chestnut	People's Committee – Distric Trùng Khánh
27	6-2010-00006	6-00027	10.08.2011	Bà Đen	Sugar Apple	Department of Science and Technology of province Tây Ninh
28	6-2010-00005	6-00028	13.10.2011	Nga Sơn	Sedge	People's Committee – Distric Nga Sơn
29	6-2009-00006	6-00029	13.10.2011	Trà My	Cinnamon Bark	Department of Science and Technology of province Quảng Nam
30	6-2010-00001	6-00030	07.02.2012	Ninh Thuận	Grapes	Department of Science and Technology of province Ninh Thuận
31	6-2011-00002	6-00031	14.11.2012	Tân Triều	Pomelo	Department of Science and Technology of province Đồng Nai
32	6-2012-00001	6-00032	14.11.2012	Bảo Lâm	Seedless Persimmon	Department of Science and Technology of province Lạng Sơn
33	6-2012-00005	6-00033	14.11.2012	Bắc Kạn	Tangerine	Department of Science and Technology of province Bắc Kạn
34	6-2009-00003	6-00034	30.11.2012	Yên Châu	Round-shaped mango	Department of Science and Technology of province Sơn La
35	6-2011-00005	6-00035	01.03.2013	Mèo Vạc	Mint honey	Department of Science and Technology of province Hà Giang
36	6-2008-00002	6-00036	29.08.2013	Bình Minh	Pomelo	Enterprise

37	6-2012-00003	6-00037	12.12.2013	Hạ Long	Fried Squid cake	People's Committee - Hạ Long city
38	6-2012-00002	6-00038	12.12.2013	Bạc Liêu	Salt	Department of Science and Technology of province Bạc Liêu
39	6-2012-00007	6-00039	18.12.2013	Luận Văn	Pomelo	People's Committee – Distric Thọ Xuân
40	6-2012-00006	6-00040	18.12.2013	Yên Tử	Yellow Mai Flower	People's Committee - Uông Bí city
41	6-2012-00004	6-00041	19.03.2014	Quảng Ninh	Bivalve mollusk	Department of Science and Technology of province Quảng Ninh
42	6-2013-00001	6-00042	18.09.2014	Isan Thái Lan	Traditional Silk	The Queen sirikit department of sericulture
43	6-2010-00004	6-00043	25.09.2014	Điện Biên	Rice	Department of Science and Technology of province Điện Biên
44	6-2008-00005	6-00044	28.10.2014	Vĩnh Kim	Lo Ren Star apple	Department of Science and Technology of province Tiền Giang
45	6-2010-00007	6-00045	28.10.2014	Quảng Trị	Pepper	Department of Science and Technology of province Quảng Trị
46	6-2013-00003	6-00046	05.11.2014	Cao Phong	Orange	Provincial People's Committee - Hòa Bình
47	6-2013-00002	6-00047	12.11.2015	Vân Đồn	Sea worm	People's Committee – Distric Vân Đồn
48	6-2015-00001	6-00048	08.06.2016	Long Khánh	Rambutan	Department of Science and Technology of province Đồng Nai
49	6-2011-00003	6-00049	16.08.2016	Ngọc Linh	Gingseng	Department of Science and Technology of province Kon Tum
50	6-2014-00002	6-00050	19.08.2016	Vĩnh Bảo	Lao tobacco	People's Committee – Distric Vĩnh Bảo
51	6-2015-00005	6-00051	10.10.2016	Thường Xuân	Cinammon	People's Committee – Distric Thường Xuân
52	6-2016-00006	6-00052	10.10.2016	Hà Giang	Organ	Department of Agriculture and Rural Development of Hà Giang province
53	6-2015-00003	6-00053	28.12.2016	Kampong Speu	Sugar Thot not (Vương quốc Cam-pu-chia)	Kompong Speu Palm Sugar Promotion Association (KSPA)
54	6-2015-00003	6-00054	28.12.2016	Kampot	Pepper (Cambodia)	Kampot Pepper Promotion Association (KPPA)
55	6-2016-00005	6-00055	23.01.2017	Hung Yên	Longan	Department of Science and Technology of province Hưng Yên
56	6-2016-00008	6-00056	05.07.2017	Quản Bạ	Seedless persimmon	People's Committee – Distric Quản Bạ
57	6-2016-00009	6-00057	28.09.2017	Xín Mần	Rice Già Dui	People's Committee – Distric Xín Mần

58	6-2016-00007	6-00058	28.09.2017	Son La	Coffee	Department of Science and Technology of province Son La
59	6-2016-00002	6-00059	24.10.2017	Ninh Thuận	Lamb	Department of Science and Technology of province Ninh Thuận
60	4-2016-00006	6-00060	08.12.2017	Thảm Dương	Sticky rice Tan Đón	People's Committee – Distric Văn Bàn
61	6-2017-00001	6-00061	22.01.2018	Mường Lò	Rice	People's Committee – Distric Nghĩa Lộ
62	6-2017-00006	6-00062	26.01.2018	Bến Tre	Pomelo	Department of Science and Technology of province Bến Tre
63	6-2017-00007	6-00063	26.01.2018	Bến Tre	Coconut	Department of Science and Technology of province Bến Tre
64	6-2014-00001	6-00064	12.02.2018	Bà Rịa –Vũng Tàu	Pepper	Department of rural development -of Bà Rịa-Vũng Tàu province
65	6-2015-00007	6-00065	12.02.2018	Ô Loan	Cockles	Department of Science and Technology of province Phú Yên
66	6-2017-00005	6-00066	13.03.2018	Bình Phước	Cashew nut	Association
67	6-2016-00003	6-00067	04.07.2018	Ninh Bình	Goat meat	Department of Agriculture and Rural Development of Ninh Bình province
68	6-2017-00004	6-00068	23.07.2018	Cao Bằng	Cooling mat	Department of Science and Technology of province Cao Bằng
69	6-2018-00001	6-00069	16.08.2018	Hà Giang	Shan Tuyet Tea	Department of Agriculture and Rural Development of Hà Giang province
70	6-2017-00002	6-00070	31.01.2019	Bà Rịa - Vũng Tàu	Longan	Department of Rural Development of Bà Rịa Vũng Tàu province
71	6-2017-00003	6-00071	31.01.2019	Cát Lở Bà Rịa - Vũng Tàu	Sugar apple	Department of Rural Development of Bà Rịa Vũng Tàu province
72	6-2018-00003	6-00072	28.02.2019	Hương Sơn	Deer Antler Velvet	People's Committee – Distric Hương Sơn
73	6-2018-00005	6-00073	12.10.2018	Hà Giang	Beef	Department of Agriculture and Rural Development of Hà Giang province
74	6-2016-00004	6-00074	27.05.2019	Đồng Giao	pineapple	People's Committee - Tam Điệp city
75	6-2018-00004	6-00075	28.05.2019	Vĩnh Châu	Onion	Department of Science and Technology of province Sóc Trăng
76	6-2018-00002	6-00076	16.09.2019	Bà Rịa	Salt	Provincial People's Committee - Bà Rịa - Vũng Tàu
77	6-2019-00004	6-00077	15.11.2019	Kỳ Sơn	Ginger	People's Committee – Distric Kỳ Sơn
78	6-2019-00006	6-00078	26.11.2019	Cao Lãnh	Mango	Department of Agriculture and Rural Development of Đồng Tháp province
79	6-2019-00008	6-00079	26.12.2019	Đăk Hà	Coffe	People's Committee – Distric Đăk Hà
80	6-2019-00010	6-00080	11.05.2020	Cái Mon	Durian	Department of Science and Technology of province tỉnh Bến Tre
81	6-2019-00011	6-00081	29.06.2020	Lý Sơn	Garlic	People's Committee – Distric Lý Sơn

82	6-2019-00009	6-00082	10.07.2020	An Thịnh	Garlic	People's Committee – Distric Lương Tài
83	6-2020-00001	6-00083	20.07.2020	Lục Nam	Deer skin	People's Committee – Distric Lục Nam
84	6-2019-00005	6-00084	07.08.2020	Vị Xuyên	Cardamom	People's Committee – Distric Vị Xuyên
85	6-2019-00013	6-00085	30.09.2020	Châu Thành Long An	Dragon fruit	Department of Science and Technology of province Long An
86	6-2020-00002	6-00086	30.09.2020	Hàm Yên	Orange	People's Committee – Distric Hàm Yên
87	6-2020-00003	6-00087	05.11.2020	Phú Yên	Lobster	Department of Science and Technology of province Phú Yên
88	6-2019-00014	6-00088	13.11.2020	Khả Linh	Pomelo	People's Committee – Distric Yên Bình
89	6-2020-00005	6-00089	23.11.2020	Văn Chấn	Trionychidae	People's Committee – Distric Văn Chấn
90	6-2020-00006	6-00090	23.11.2020	Cổ Lũng – Bá Thước	Duck	People's Committee – Distric Bá Thước
91	6-2020-00004	6-00091	23.11.2020	Cù Lao Chàm – Hội An	Edible Bird's net	People's Committee - Hội An city
92	6-2020-00009	6-00092	23.11.2020	Cầu Đúc	Pineapple	Department of Agricultural, Forestry and Fishery Product quality Management of Hậu Giang province
93	6-2020-00008	6-00093	23.11.2020	Mang Yang	Rice Ba Châm	People's Committee – Distric Mang Yang - tỉnh Gia Lai
94	6-2020-00011	6-00094	23.11.2020	Trà Bồng	Cinammon	Department of Science and Technology of province Quảng Ngãi
95	6-2020-00010	6-00095	03.12.2020	Vĩnh Châu	Artemia	Department of Science and Technology of province Sóc Trăng
96	6-2020-00014	6-00096	03.12.2020	Huế	Cajeput essencial oil	Provincial People's Committee - Thừa Thiên Huế
97	6-2019-00001	6-00097	25.12.2020	Kagoshima Wagyu/Kagos hima, Kuroushi/Thịt bò Kagoshima	Beef	Kagoshima Prefectural Beef Cattle Promotion Council
98	6-2020-00013	6-00098	25.12.2020	Mường Khương – Bát Xát	Rice Sẻng Cù	Department of Science and Technology of province Lào Cai
99	6-2019-00012	6-00099	28.12.2020	Yên Bái	Bammo shoots Bát Độ	People's Committee – Distric Trấn Yên
100	6-2020-00017	6-00100	29.12.2020	Tú Lệ	Sticky rice nếp	People's Committee – Distric Văn Chấn
101	6-2020-00007	6-00101	29.12.2020	Mù Cang Chải	Honey	People's Committee – Distric Mù Cang Chải

102	6-2020-00019	6-00102	14.04.2021	Bến Tre	Sea crab	Department of Science and Technology of province Bến Tre
103	6-2020-00015	6-00103	19.04.2021	Bến Tre	Lobster	Department of Science and Technology of province Bến Tre
104	6-2020-00019	6-00104	23.04.2021	Na Hang	Tea	People's Committee – Distric Na Hang
105	6-2019-00002	6-00105	29.04.2021	Hà Giang	Cyprinus carpio	Department of Agriculture and Rural Development of Hà Giang province
106	6-2020-00016	6-00106	29.04.2021	Bắc Kạn	Dong Vermicelli	Department of Science and Technology of province Bắc Kạn
107	6-2019-00003	6-00107	14.06.2021	ICHIDA GAKI/ICHIDA A KAKI/ HÔNG ICHIDA	persimmon	Minami Shinshu Agricultural Cooperative Association
108	6-2020-00012	6-00108	02.08.2021	Núi Dành	Gingseng	People's Committee – Distric Tân Yên
109	6-2021-00005	6-00109	15.09.2021	Soi Hà	Pomelo	People's Committee – Distric Yên Sơn
110	6-2020-00022	6-00110	30.09.2021	Cà Mau	Lobster	Department of Science and Technology of province Cà Mau
111	6-2021-00001	6-00111	09/11/2021	Đắk Nông	Pepper	Department of Science and Technology of province Đắk Nông
112	6-2021-00004	6-00112	09/11/2021	Phình Hồ	Tea	People's Committee – Distric Trạm Tấu
113	6-2016-00001	6-00113	09/11/2021	Khánh Hòa	Babylonia areonata	Association
114	6-2017-00009	6-00114	24/11/2021	Phechabun	Tamarindus indica	Phetchabun Province (Phetchabun Provincial Government)
115	6-2021-00003	6-00115	27/12/2021	Chư Sê	Pepper	People's Committee – Distric Chư Sê
116	6-2021-00006	6-00116	08/6/2022	Cà Mau	Crab	Department of Science and Technology of province Cà Mau
117	6-2017-00008	6-00117	05/08/2022	Lam Phun	Longan	Lamphun Provincial Administrative Organization
118	6-2021-00007	6-00118	05/08/2022	Bến Kè	Purple yam	People's Committee – Distric Thanh Hóa
119	6-2018-00006	6-00119	17/08/2022	MIYAGI SALMON	Salmon	Miyagi Coho Salmon Promotion Association
120	6-2019-00007	6-00120	03/10/2022	TEQUILA	Wine	CONSEJO REGULADOR DEL TEQUILA, A.C
121	6-2020-00020	6-00121	04/11/2022	Văn Chấn	Organ	People's Committee – Distric Văn Chấn
122	6-2021-00010	6-00122	04/11/2022	Suối Giàng Văn Chấn	Tea Shan tuyết	People's Committee – Distric Văn Chấn

123	6-2007-00003	6-00123	10/11/2022	NAPA VALLEY	Wine	NAPA VALLEY VINTNERS
124	6-2022-00004	6-00124	10/11/2022	Bến Tre	Mango	Department of Science and Technology of province Bến Tre
125	6-2021-00011	6-00125	10/11/2022	Gia Lai	Coffee	Department of Science and Technology of province Gia Lai
126	6-2022-00002	6-00126	19/01/2023	Quảng Trị	Tea	Department of Science and Technology of province Quảng Trị
127	6-2022-00009	6-00127	09/02/2023	Lạng Sơn	Mesona chinesis	Department of Agriculture and Rural Development of Lạng Sơn province
128	6-2022-00012	6-00128	20/02/2023	Na Hang	Corn wine	People’s Committee – Distric Na Hang
129	6-2022-00008	6-00129	17/04/2023	Vân Thủy	Honey	People’s Committee – Distric Chi Lăng
130	6-2021-00009	6-00130	05/06/2023	Bắc Kạn	Duck	Department of Science and Technology of province Bắc Kạn
131	6-2022-00003	6-00131	28/11/2023	Bến Tre	Rambutan	Department of Science and Technology of province Bến Tre
132	6-2022-00016	6-00132	26/12/2023	La Tinh Hoài Đức	Sugar pomelo	People’s Committee – Distric Hoài Đức
133	6-2021-00008	6-00133	18/01/2024	Bến Lức Long An	Seedless lemon	Department of Agriculture and Rural Development of Long An province
134	6-2023-00008	6-00134	18/01/2024	Huế	Hoàng Mai (yellow Mai Flower)	Department of Science and Technology of province Thừa Thiên Huế
135	6-2023-00003	6-00135	18/01/2024	Huế	Mango plum	Department of Science and Technology of province Thừa Thiên Huế
136	6-2022-00013	6-00136	25/01/2024	Bình Định	Yellow Mai tree	Department of Science and Technology of province Bình Định
137	6-2022-00022	6-00137	05/02/2024	Thanh Phú	Rice	Department of Science and Technology of province Bến Tre

Source: ipvietnam.gov.vn¹⁴

The given table shows that the vast majority of GI-labelled products have been registered by public authorities and non-agricultural GIs have not yet received the attention they deserve as only 2 out of 137 GIs were classified as non-agricultural product (the Hue conical hats (non la Hue) and Cao Bang bamboo mats). This

¹⁴ List of GI-protected products in Vietnam, available at https://www.ipvietnam.gov.vn/en_US/web/english/list-of-protected-gis-in-viet-nam (accessed on November 2, 2025).

situation demonstrates the lack of focus on non-agricultural GIs in a country that is home to 3,597 traditional craft villages.¹⁵

Furthermore, GIs in Vietnam have currently been established and managed based on various level of inspection, enforcement, traceability rules. For instance, the Binh Phuoc cashew nut has been protected as a GI since 2018¹⁶ and is owned by the People's Committee of Binh Phuoc province, with management handled by the Department of Science and Technology¹⁷. In contrast, the Binh Thuan Dragon Fruit, which received its protection certificate in 2020¹⁸ is managed by the Binh Thuan dragon fruit association¹⁹. The divergences in the GI management systems across various provinces not only reflect the absence of a unified national management and enforcement for GIs, but also demonstrate the varying level of participation and engagement of key stakeholders, particularly GI producers, in the elaborating and developing of GI specifications.

Additionally, the administrative restructuring that took place in April 2025 has negatively impacted the situation for the Vietnamese GIs. Specifically, according to the Article 1(2) of the Resolution No.76/2025/UBTVQH15, dated April 14, 2025, the rearrangement of province-level administrative divisions means merging provinces with other provinces to establish new provinces, or merging provinces with centrally-affiliated cities to establish new centrally-affiliated cities, as approved by the competent authorities, in order to reduce the number of administrative divisions, increase their scale, and expand development space. As a result of this restructuring, operation of district-level administrative divisions nationwide shall be terminated from July 01, 2025²⁰, leading to the removal of

¹⁵ Nga, T H.; Nguyen, N K H, *Protection of non-agricultural geographical indications under EU law: implications for the EVFTA and compatibility with Vietnam's intellectual property legislation*, TalTech Journal of European Studies, 2025, 25-39, p.36, available at <https://doi.org/10.2478/bjes-2025-0018>.

¹⁶ Decision 673/QĐ-SHTT of the National Office of Intellectual Property, granting the GI registration Certificate No.00066 for cashew nut from Binh Phuoc, https://ipvietnam.gov.vn/web/english/news-events/-/asset_publisher/ZMuTgR44COLR/content/geographical-indication-of-binh-phuoc-for-cashew-nut-protected?utm_source=chatgpt.com (accessed on November 8, 2025).

¹⁷ Article 6(3) of Decision No. 2065/2018/QĐ-UBND issued by the People's Committee of Binh Phuoc province to govern how the GI is used, controlled and maintained.

¹⁸ Decision 1577/QĐ-SHTT of the National Office of Intellectual Property, granting the GI registration Certificate No. 00006 for dragon fruit from Binh Thuan, <https://ipvietnam.gov.vn/documents/20182/1185430/0006.pdf/cd3b6d4a-1779-460a-8137-4ea228f3564d> (accessed November 15,2025) .

¹⁹ Article 4(1) of Decision No. 76/2015/QĐ-UBND issued by the People's Committee of Binh Thuan province to govern how Binh Thuan GI is used and managed.

²⁰ Article 2 (2), Resolution No.203/2025/QH15 amendments to certain articles of the Constitution of the Socialist Republic of Vietnam.

numerous provinces and cities from the administrative map. Consequently, many GIs pertained to such eliminated provinces face the risk of confusion regarding the origin of their products, potentially damaging their reputation. For example, Ben Tre province, which had protection for its green-skinned pomelos originating from six districts - Chau Thanh, Giong Trom, Mo Cay Bac, Mo Cay Nam, Cho Lach, Binh Dai, and Ben Tre city²¹ - will no longer exist as a separate administrative unit. It has been dissolved and merged with Vinh Long and Tra Vinh provinces to form a new entity called Vinh Long province. According to the Article 10 of the Resolution No. 190/2025/QH15 providing regulations on handling certain issues related to the reorganization of the state apparatus, the applicant, the holder of the protection certificate, or person authorized by State to exercise the right to register GIs has the right to request the National Office of Intellectual Property to amend or supplement the GI application or protection certificate to record changes in the address of the applicant, the owner of GI protection certificate, or the GI management organization due to the rearrangement of administrative units. However, a significant concern arises when the name Ben Tre is removed. This core element, which signifies the origin of the product, will no longer be present, potentially leading to confusion and infringing activities.

5. RECOMMENDATIONS FOR MAINTENANCE AND DEVELOPMENT OF THE VIETNAMESE GI SYSTEM

Firstly, the Vietnamese government should take action to provide producers of GI-protected products more opportunities to express their opinions on the elaboration, protection and management of GI. This study supports the approach proposed by Marie-Vivien²² that Vietnam should adopt the EU's bottom-up approach to GIs, allowing producer groups to engage actively and prominently in the elaboration of product specifications, application for GI protection and GI management. This measure would also increase the awareness of producers of the importance and evaluation of GIs.

Secondly, from the EU's perspective, GI-designated product is sustainable product itself. Therefore, the EU has developed a strategy to link GI protection intrinsically

²¹ Decision 297/QĐ-SHTT of the National Office of Intellectual Property, granting the GI registration Certificate No. 00062 for green-skinned pomelos from Ben Tre province, <https://ipvietnam.gov.vn/documents/20182/1185430/00062.pdf/3de56278-4235-4db8-bd67-b52b0ba45db9> (accessed November 21, 2025).

²² Pick, B.; Marie-Vivien, D., *Representativeness in Geographical Indications: A Comparison between the State-Driven and Producer-Driven Systems in Vietnam and France*, Sustainability, 2021, 1-16, p.16, available at <https://doi.org/10.3390/su13095056>.

to sustainable development objectives. It is recommended that Vietnamese IP law be amended to introduce a provision requiring GI producers to submit periodic sustainability reports. In that way, products labelling GIs originating from Vietnam would be better equipped to satisfy the EU market's sustainability requirements, thereby enhancing their prospects for obtaining GI protection in Europe.

With regard to craft and industrial products, the EU has recently expanded its GI framework by introducing regulations governing the protection of non-agricultural products.²³ Meanwhile, Vietnam continues to concentrate predominantly on agricultural GIs. It is therefore necessary for Vietnam to learn from the EU's experience in developing the distinct legal framework for the protection of craft and industrial products. This approach could contribute to safeguarding traditional heritage while also mitigating the risk of the disappearance of traditional craft villages in Vietnam.

Lastly, the recommendation for minimizing the ambiguity concerning the GI-labelled products whose characteristics are associated with provinces that have been merged is that the competent authorities should ensure that registration application and related documentation are duly updated to reflect such administrative changes. At the same time, the name of products that have previously been granted geographical indications protection should be retained; however, the continue legal validity of those GIs should be clarified to ensure legal certainty and transparency.

6. CONCLUSION

The paper has examined the current state of Vietnam's GI legal framework and the actual state of Vietnam's GI system. Although the Vietnamese regulations on GIs are broadly aligned with international standards, the involvement of producers in the elaboration, management and enforcement is still limited due to the continuance of a predominantly top-down governance model.

Furthermore, the absence of explicit sustainability provisions in Vietnam's GI legislation reveals critical gap in light of global trends. In order to learn from the way EU responses to sustainability requirements, Vietnam should incorporate sustainability requirements into its GI legal framework. That would enhance the

²³ Regulation (EU) 2023/2411 of the European Parliament and of the Council on the protection of geographical indications for craft and industrial products.

international competitiveness of Vietnamese GI products, particularly within the EU market.

The research also highlights the underdevelopment of non-agricultural GIs in Vietnam, despite the country's rich tradition handicraft and craft villages. Developing a distinct legal framework for non-agricultural GIs in Vietnam could contribute significantly to not only increase the number of craft and industrial products protected as GI, but also preserve traditional heritage.

Finally, the administrative restructuring in Vietnam presents new legal and practical challenges for the maintenance of GI protection. Ensuring that registration dossiers are updated to reflect the administrative changes, while simultaneously clarifying the continued legal validity of existing GIs, is essential to safeguard legal certainty and prevent confusion regarding product origin.

Overall, the study concludes that Vietnam's GI system has achieved important milestones but requires structural refinement, stronger producer engagement, sustainability integration, and adaptive administrative mechanisms. Drawing lesson from the EU, experience does not imply simple transplantation; rather, it requires selective adaption consistent with Vietnam's social-economic conditions.

REFERENCES

BOOKS AND ARTICLES

1. Adinolfi, F.; Vecchio, Y.; Masi, M.; Mastandrea, G.; Lambertini, G.; De Castro, P., (2024). The reform of EU geographical indications: A look at the newly approved Regulation, AIMS AGRICULTURE AND FOOD, 2024, 693-698, p., available at <https://doi.org/10.3934/AGRFOOD.2024037>
2. Nguyen, S L.; Le, V A., Diffusion of Geographical Indication Law in Vietnam: "Journey To The West", IIC, 2023, 176-199, p. 179, available at <https://doi.org/10.1007/s40319-023-01289-9>
3. Nga, T H.; Nguyen, N K H, Protection of non-agricultural geographical indications under EU law: implications for the EVFTA and compatibility with Vietnam's intellectual property legislation, TalTech Journal of European Studies, 2025, 25-39, p30, available at <https://doi.org/10.2478/bjes-2025-0018>
4. Pick, B.; Marie-Vivien, D., Representativeness in Geographical Indications: A Comparison between the State-Driven and Producer-Driven Systems in Vietnam and France, Sustainability, 2021, 1-16, p.16, available at <https://doi.org/10.3390/su13095056>

LEGAL ACTS

1. Decision 673/QD-SHTT of the National Office of Intellectual Property, granting the GI registration Certificate No.00066 for cashew nut from Binh Phuoc, available at https://ipvietnam.gov.vn/web/english/news-events/-/asset_publisher/ZMuTgR44COLR/content/geographical-indication-of-binh-phuoc-for-cashew-nut-protected?utm_source=chatgpt.com (accessed November 8, 2025)
2. Article 6(3) of Decision No. 2065/2018/QD-UBND issued by the People's Committee of Binh Phuoc province to govern how the GI is used, controlled and maintained.
3. Decision 1577/QD-SHTT of the National Office of Intellectual Property, granting the GI registration Certificate No. 00006 for dragon fruit from Binh Thuan, available at <https://ipvietnam.gov.vn/documents/20182/1185430/0006.pdf/cd3b6d4a-1779-460a-8137-4ea228f3564d> (accessed November 15,2025)
4. Decision No. 76/2015/QD-UBND issued by the People's Committee of Binh Thuan province to govern how Binh Thuan GI is used and managed.
5. Resolution No.203/2025/QH15 amendments to certain articles of the Constitution of the Socialist Republic of Vietnam
6. Decision 297/QD-SHTT of the National Office of Intellectual Property, granting the GI registration Certificate No. 00062 for green-skinned pomelos from Ben Tre province, available at <https://ipvietnam.gov.vn/documents/20182/1185430/00062.pdf/3de56278-4235-4db8-bd67-b52b0ba45db9> (accessed November 21, 2025)

NETWORK RESOURCE

1. Chapter 12, The EU-Vietnam Free Trade Agreement, available at https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/viet-nam/eu-viet-nam-agreements/texts-agreements_en, (accessed on September 4, 2025)
2. Geographical indications and quality scheme explained, available at https://agriculture.ec.europa.eu/farming/geographical-indications-and-quality-schemes/geographical-indications-and-quality-schemes-explained_en#pdo, (accessed on September 10, 2025)
3. List of GI-protected products in Vietnam, available at https://www.ipvietnam.gov.vn/en_US/web/english/list-of-protected-gis-in-viet-nam, (accessed on November 2, 2025)

